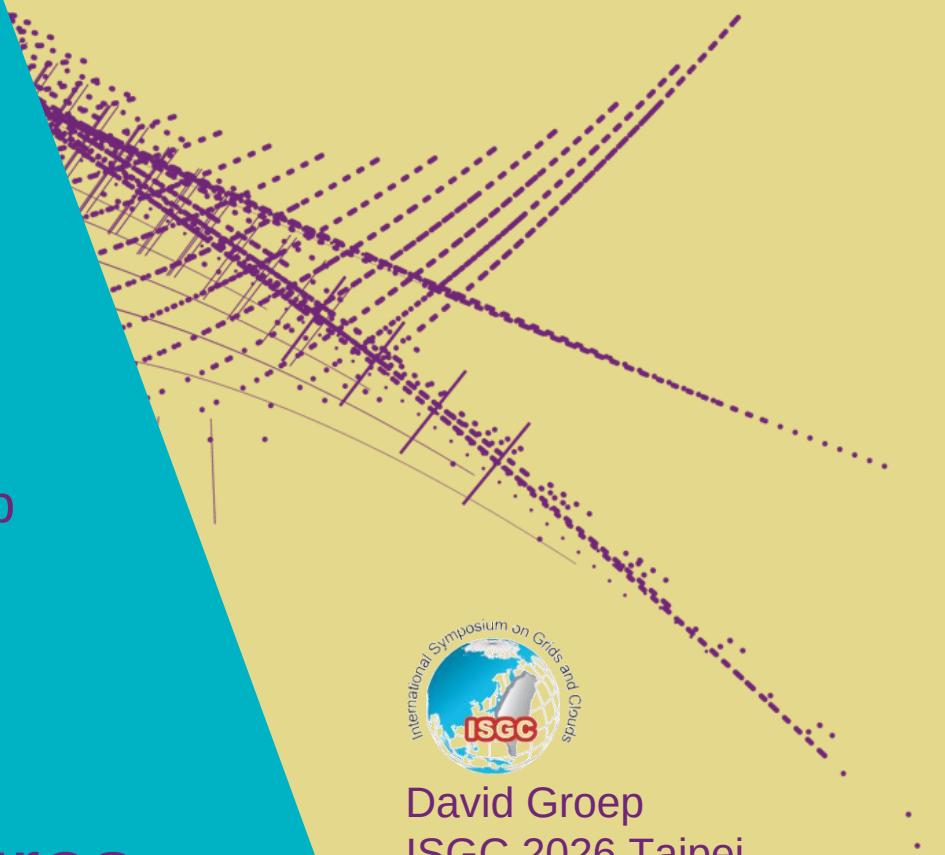
Nikhef

Maastricht University

EGI-CSIRT Security Training Workshop



IT Security for complex infrastructures

David Groep

ISGC 2026 Taipei

March 2026

Remember the days when computing was safe & simple

An IBM Portable PC in use by early 1985

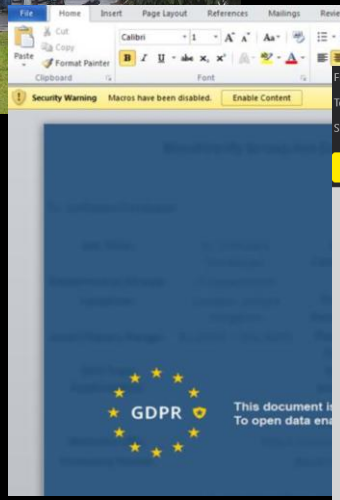
… and then they got networked …

Nikhef user room H1.37 – terminal stations in the early 1990's – image source: Nikhef

Today we have more people, more computing, more …

a small part of the CMS collaboration in 2017, photo credit CERN on behalf the CMS collaboration, CMS-PHO-PUBLIC-2017-004-3

… and many more risks



From Prof Dr M.H.M. Winands <artisanhairs789@gmail.com>
To david.groep@maastrichtuniversity.nl
Subject
DKIM Valid (Signed by gmail.com)

Hello are you available? I need your assistance urgently

Prof Dr M.H.M. Winands

Professor in Machine Reasoning
Chair of the Department of Advanced Computing Sciences
Dept. of Advanced Computing Sciences

From Loopia AB <faktururony@neverlandsodermalm.se>
To ops-management@rcauth.eu 2023-12-27, 22:13
Subject **Din betalning gick inte igenom**

To protect your privacy, Thunderbird has blocked remote content in this message. Options

Din betalning gick inte igenom

Betalningen för faktura (691206380) gick ej att genomföra då kortet passerat förfallodatum.

Beskrivning	Delsumma
Webbhotell, Privatpaket	1 188,00
Totalt	**1 188,00**
Moms (25%)	**297,00**
	Att betala: 1 485,00 SEK

Betala direkt med kort

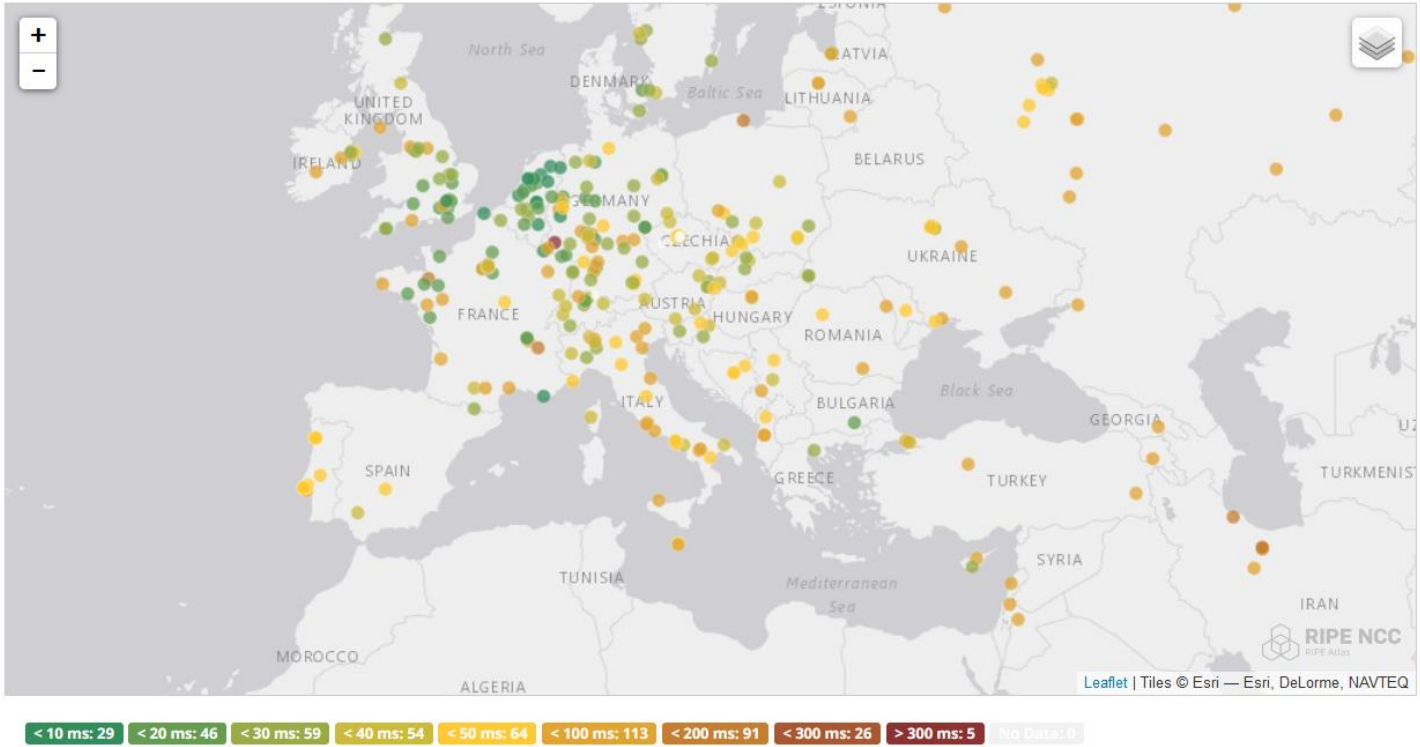
Thanks to: https://labs.f-secure.com/assets/BlogFiles/f-secureLABS-tlp-white-lazarus-threat-intel-report2.pdf, uni-Giessen, Universiteit Maastricht, SURFnet, … and a bunch of phishers

And not all risks are criminal, but still infrastructure risks

you may need some investment in BC/DR – and Northgate Plc. indeed did & managed to pay on time

CHEP2018 [EPJ Web of Conferences 214, 09008 (2019) https://doi.org/10.1051/epjconf/201921409008], imagery: HSE, https://www.hse.gov.uk/comah/buncefield/

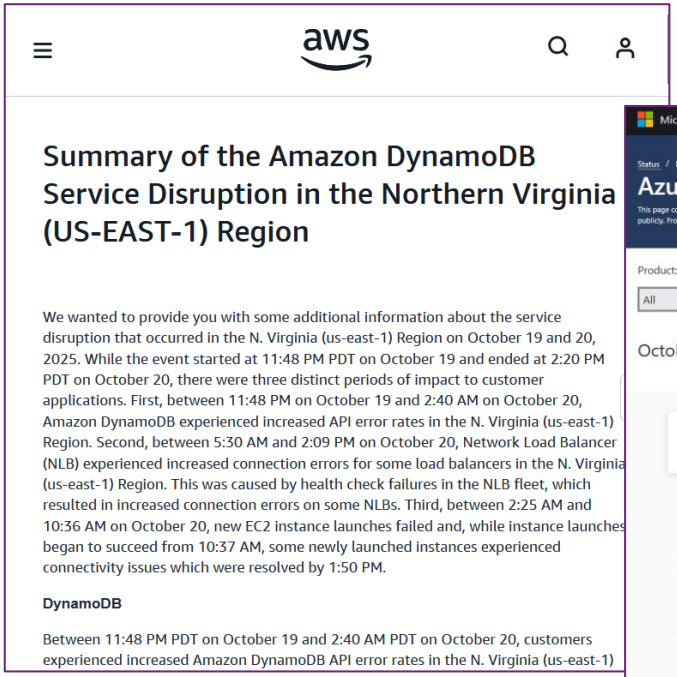
And while CDNs and Cloud may be part of a solution …



RCauth.eu: anycasted identity token translation service distributed across Nikhef, GRNET, and RAL

map: RIPE NCC RIPE Atlas - 500 probes, distributed across Europe (https://atlas.ripe.net/measurements/50949024/)

But abstractions are leaky and dependencies unfathomable …



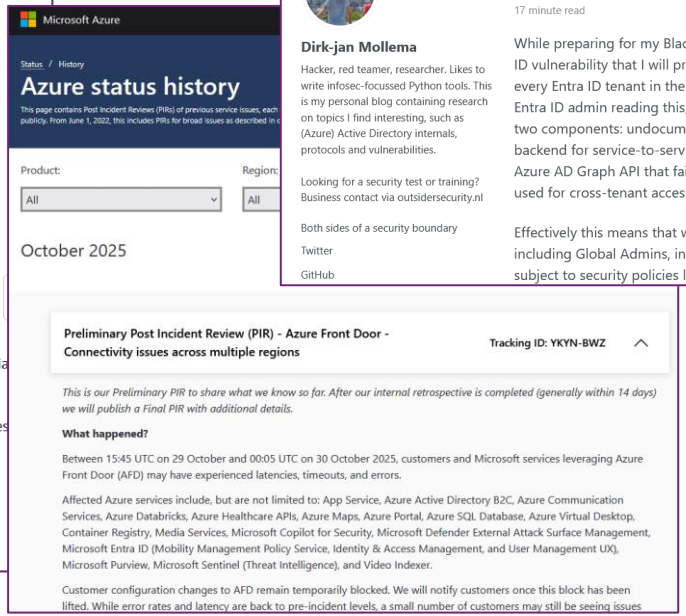
aws

Summary of the Amazon DynamoDB Service Disruption in the Northern Virginia (US-EAST-1) Region

We wanted to provide you with some additional information about the service disruption that occurred in the N. Virginia (us-east-1) Region on October 19 and 20, 2025. While the event started at 11:48 PM PDT on October 19 and ended at 2:20 PM PDT on October 20, there were three distinct periods of impact to customer applications. First, between 11:48 PM on October 19 and 2:40 AM on October 20, Amazon DynamoDB experienced increased API error rates in the N. Virginia (us-east-1) Region. Second, between 5:30 AM and 2:09 PM on October 20, Network Load Balancer (NLB) experienced increased connection errors for some load balancers in the N. Virginia (us-east-1) Region. This was caused by health check failures in the NLB fleet, which resulted in increased connection errors on some NLBs. Third, between 2:25 AM and 10:36 AM on October 20, new EC2 instance launches failed and, while instance launches began to succeed from 10:37 AM, some newly launched instances experienced connectivity issues which were resolved by 1:50 PM.

DynamoDB

Between 11:48 PM PDT on October 19 and 2:40 AM PDT on October 20, customers experienced increased Amazon DynamoDB API error rates in the N. Virginia (us-east-1)



Microsoft Azure

Status / History

Azure status history

This page contains Post Incident Reviews (PIRs) of previous service issues, each publicly. From June 1, 2022, this includes PIRs for broad issues as described in

Product: All

Region: All

October 2025

Preliminary Post Incident Review (PIR) - Azure Front Door - Connectivity issues across multiple regions

Tracking ID: YKYN-BWZ

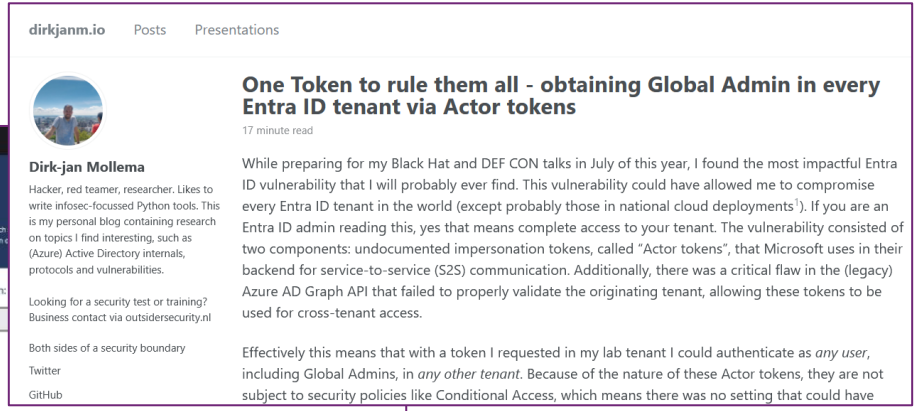
This is our Preliminary PIR to share what we know so far. After our internal retrospective is completed (generally within 14 days) we will publish a Final PIR with additional details.

What happened?

Between 15:45 UTC on 29 October and 00:05 UTC on 30 October 2025, customers and Microsoft services leveraging Azure Front Door (AFD) may have experienced latencies, timeouts, and errors.

Affected Azure services include, but are not limited to: App Service, Azure Active Directory B2C, Azure Communication Services, Azure Databricks, Azure Healthcare APIs, Azure Maps, Azure Portal, Azure SQL Database, Azure Virtual Desktop, Container Registry, Media Services, Microsoft Copilot for Security, Microsoft Defender External Attack Surface Management, Microsoft Entra ID (Mobility Management Policy Service, Identity & Access Management, and User Management UX), Microsoft Purview, Microsoft Sentinel (Threat Intelligence), and Video Indexer.

Customer configuration changes to AFD remain temporarily blocked. We will notify customers once this block has been lifted. While error rates and latency are back to pre-incident levels, a small number of customers may still be seeing issues



dirkjanm.io Posts Presentations

One Token to rule them all - obtaining Global Admin in every Entra ID tenant via Actor tokens

17 minute read

Dirk-jan Mollema

Hacker, red teamer, researcher. Likes to write infosec-focussed Python tools. This is my personal blog containing research on topics I find interesting, such as (Azure) Active Directory internals, protocols and vulnerabilities.

Looking for a security test or training? Business contact via outsidersecurity.nl

Both sides of a security boundary

Twitter

GitHub

While preparing for my Black Hat and DEF CON talks in July of this year, I found the most impactful Entra ID vulnerability that I will probably ever find. This vulnerability could have allowed me to compromise every Entra ID tenant in the world (except probably those in national cloud deployments[1]). If you are an Entra ID admin reading this, yes that means complete access to your tenant. The vulnerability consisted of two components: undocumented impersonation tokens, called "Actor tokens", that Microsoft uses in their backend for service-to-service (S2S) communication. Additionally, there was a critical flaw in the (legacy) Azure AD Graph API that failed to properly validate the originating tenant, allowing these tokens to be used for cross-tenant access.

Effectively this means that with a token I requested in my lab tenant I could authenticate as *any user*, including Global Admins, in *any other tenant*. Because of the nature of these Actor tokens, they are not subject to security policies like Conditional Access, which means there was no setting that could have

*One month worth of *aaS events*

https://aws.amazon.com/message/101925/, https://azure.status.microsoft/en-us/status/history/, https://dirkjanm.io/obtaining-global-admin-in-every-entra-id-tenant-with-actor-tokens/

Distributed research computing, collaborating for decades

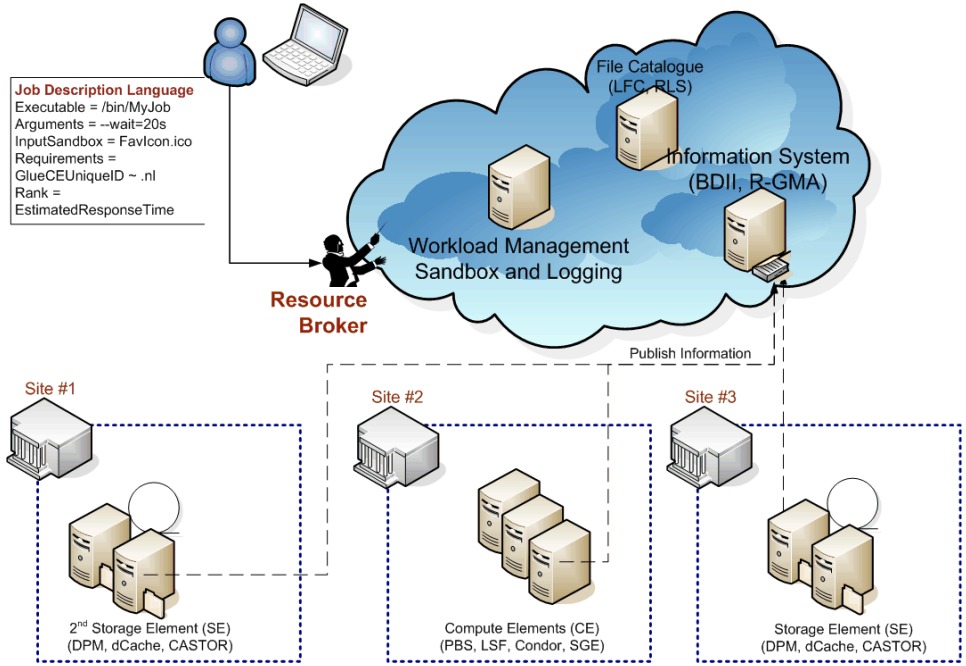
Finding mechanisms to collaborate
beyond the canonical ~150 people (“Dunbar’s number”)
but what we built, may be unique for
our ‘high-trust’ research community … or an example for others

Worldwide LHC
Computing Grid (~ 2024)
~ 1.4 million CPU cores
~ 1500 Petabyte
disk + archival

170+ institutes
42+ countries
13 ‘Tier-1 sites’
some multi-community:
NL-T1 @ SURF & Nikhef

Earth background: Google Earth; Data and compute animation: STFC RAL for WLCG and EGI.eu; Data: https://home.cern/science/computing/grid ;
LHC Computing Grid: wlcg.web.cern.ch, EGI: www.egi.eu; ACCESS CI: https://access-ci.org/, NL-T1 and FuSE: fuse-infra.nl, https://www.surf.nl/en/research-it

Beyond the enterprise egg shell …



Interoperable cloud? Compare OGF's OCCI WG GFD.221 (https://www.ogf.org/documents/GFD.221.pdf) with e.g. Amazon S3 API or the OwnCloud CS3 interfaces

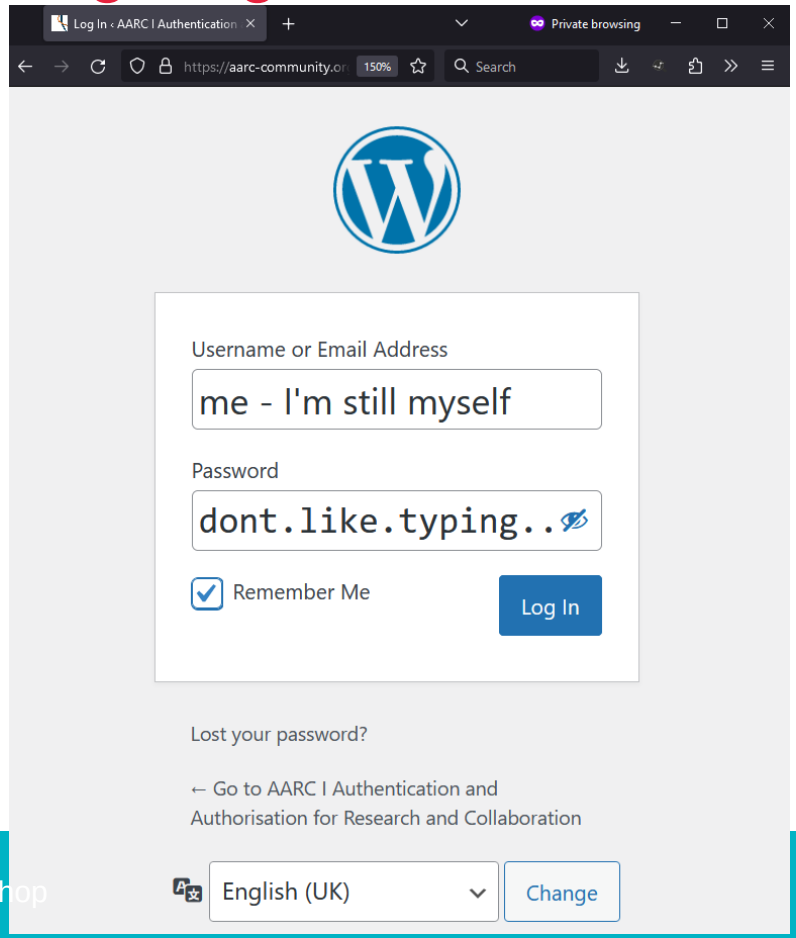
When you are asked to login again…~12 000 x 170+ times?

Authentication

demonstrating ‘you are you’

- ***authenticator***
  ‘you’ remains same ‘you’

- **vetted *identity***
  ‘you’ can be pseudonymous
  ‘you’ can be a vetted person



Self-asserted or ‘pseudonymous’ often not enough

state of EU DataGrid and HEP computing in ~2000

NIKHEF
NATIONAAL INSTITUUT VOOR KERNFYSICA EN HOGE-ENERGIEFYSICA

Guest / students form (pleas

1. This form is completed in connection with:

☐ work experien
☐ otherwise, vis

CERN/User Registration

CERN COMPUTER CENTRE - US

http://cern.ch/it/documents/ComputerUsage/CompA

To be returned to the User Registration box at the en
completed by a user who requires a computer accou
Department, and is not yet registered in another grou

To be completed by the User :

It is **MANDATORY** to provide the following infor
treated confidentially and only be used for ensuring
Supply name as registered by the Users' Off
FAMILY NAME(S): ……
FIRST NAME(S) : ……
SEX [M] [F] BIRTHDATE: Day …… Month …… Year ……
HOME INSTITUTE/FIRM: ……
NATIONALITY: ……..*CERN SUPERVISOR……
*CERN DEPARTMENT: . . . . . *CERN ID NUMBER (as on CERN card)……..

To be completed by the Group Administrator:

Fermilab

For Office Use Only

ID:	Action:	ID Exp:	
Insurance:	Medical:	Safety:	
Computer:	Stkrm:	Family:	
NON-473:	Sensitive:	Verifier:	Date:

Name:

Last	First	Middle
SWIETZER	JOHN	JAMES

University or Institution Name: Telephone:

FLORIDA STATE UNIVERSITY	850-644-XXXX

Experiment/Department:

Exp. / Dept.	Spokesperson	Home Institution Contact	Contact Telephone
D0	WOMERSLEY/WEERTS	SHARON HAGOPIAN	850-644-4777

Can we scale better with an ‘federated’ Authentication and Authorisation Infrastructure (‘AAI’)

with one service provided to several organisations in a common *federation*

we will get to authorisation in a bit …

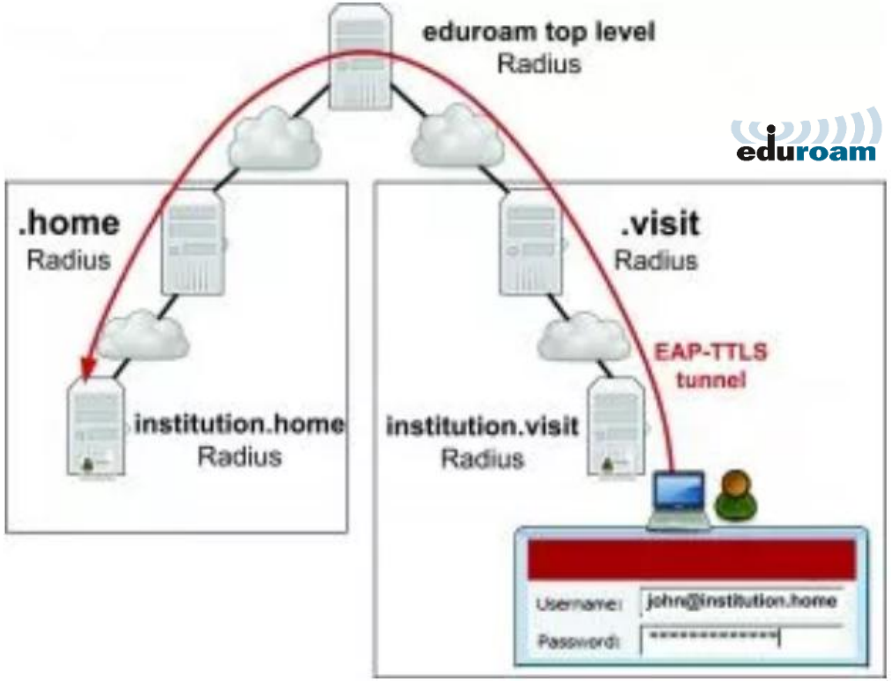
The R&E federation that was there first …

service-specific trust
between organisations

hierarchical server path, based on
a network-specific secure exchange

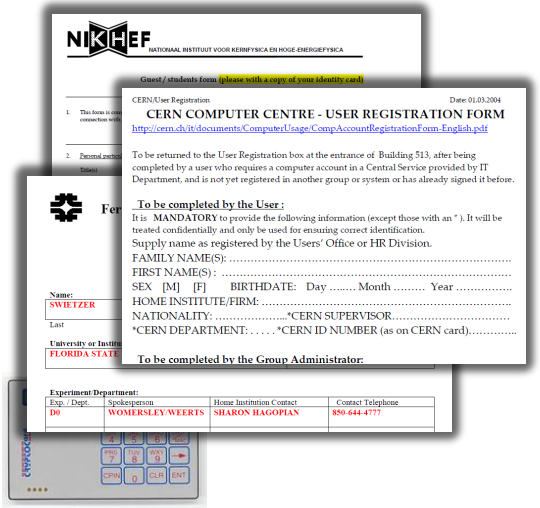
sending your credentials back
to *only* your home institution

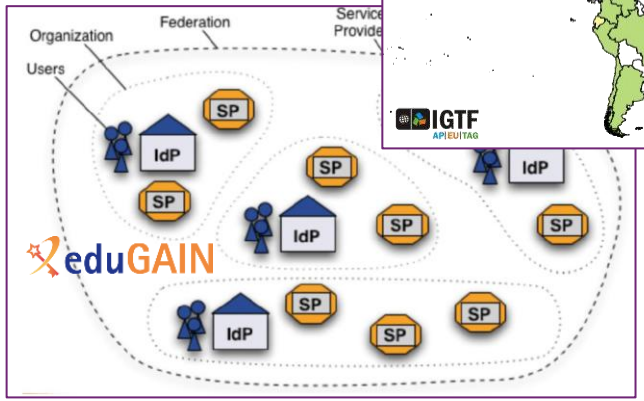
found via <anon**@domain.name**>

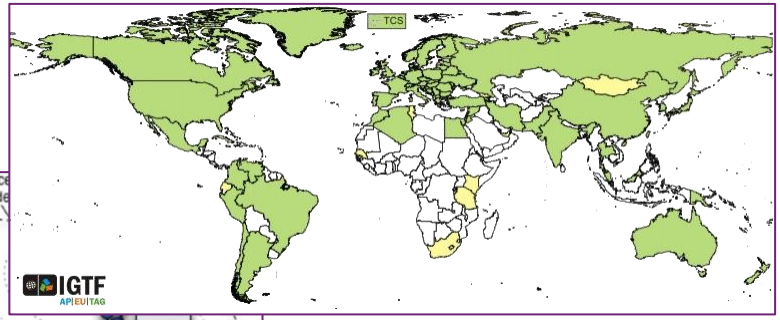


eduroam image from https://eduroam.org/how/, GEANT ; RADIUS: RC2865 https://www.rfc-editor.org/rfc/rfc2865; see also freeradius.org

We progressed a lot since 2003 with identity federation







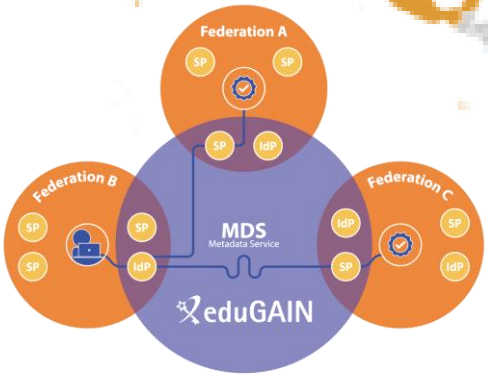
For eduGAIN federation the IdPs provide **authentication** from the home organisation, for the user-centric PKIX IGTF trust fabric, the CAs do.
Then **Service providers** perform **authorization**,
… maybe using attributes provided by the IdP. But do they get them??

Right-hand image: Shibboleth IdP federation, Lukas Hammerle, SWITCH (CH), user-centric PKI credentials: Interoperable Global Trust Federation, https://igtf.net/

78
Identity Federations

5100+
Identity Providers

3600+
Service Providers

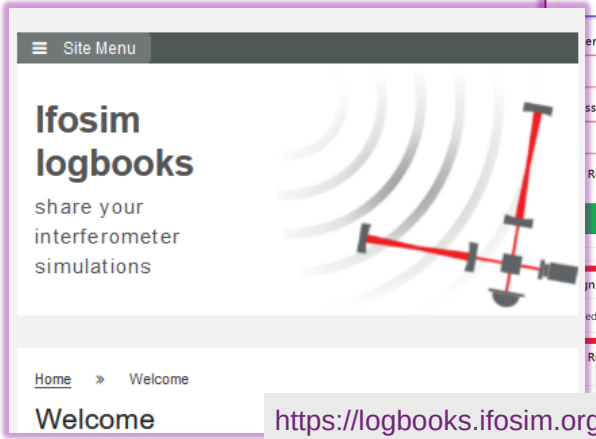


eduGAIN image: Davide Vaghetti, GARR for GN*-*, https://technical.edugain.org/

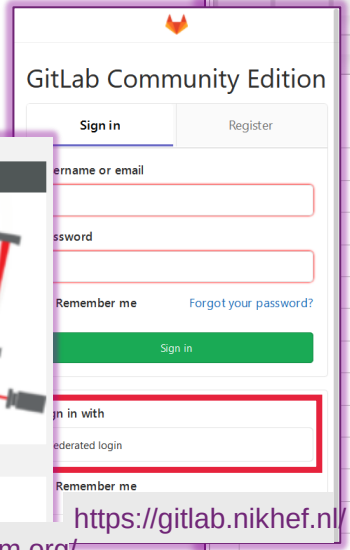
Federated Success!

Login to GW's ifosim.org, to gitlab, or … via the service proxy

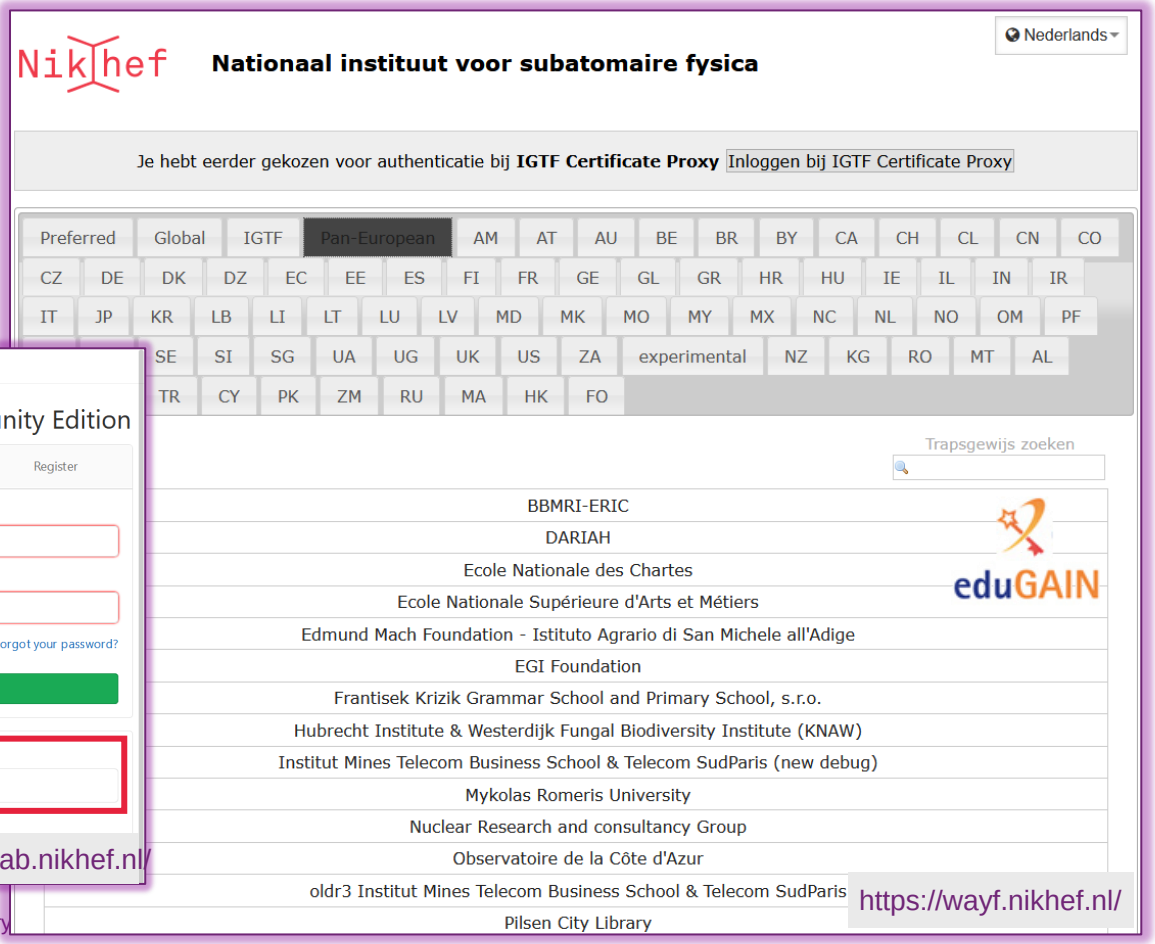
with any eduGAIN IdP for user authentication



https://logbooks.ifosim.org/



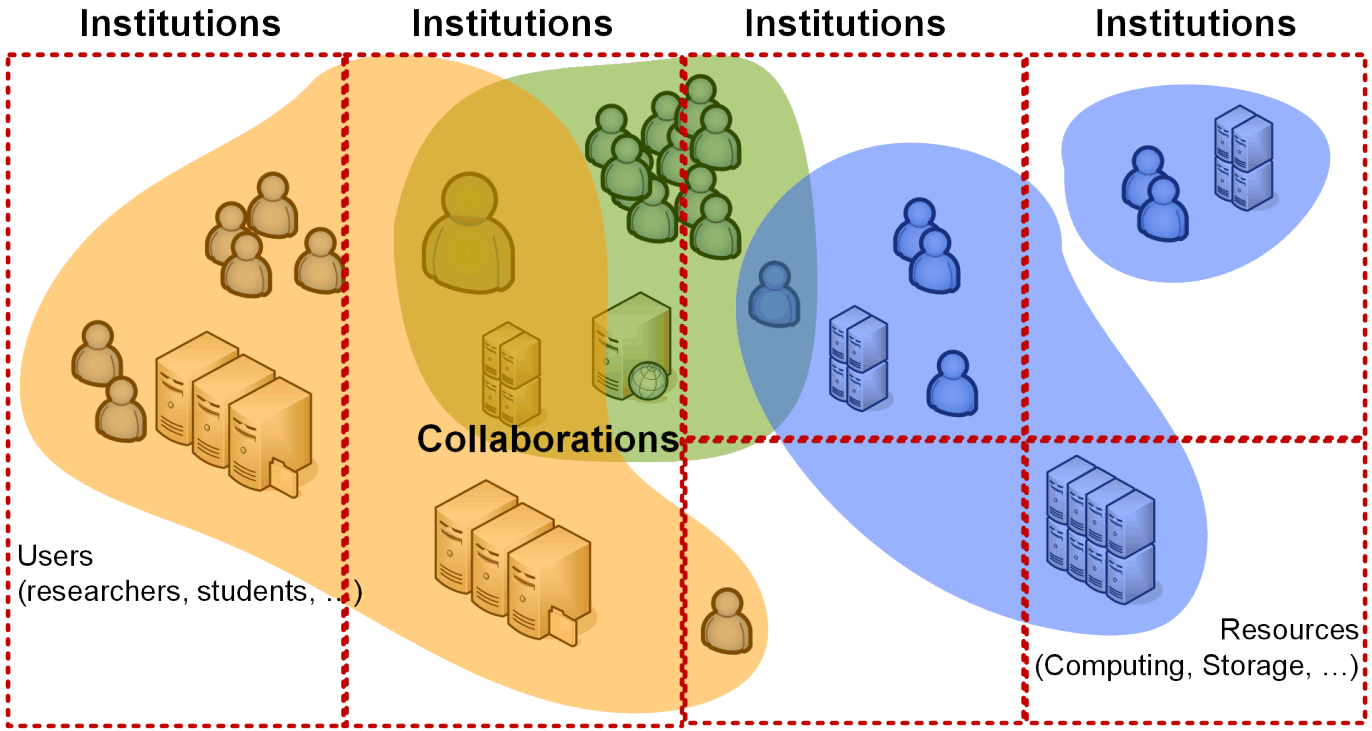
https://gitlab.nikhef.nl/



https://wayf.nikhef.nl/

ifosim federated AAI integration implementation by Mischa Sallé; per-country

Since collaborations and institutions slice in different ways



… security must bridge domains …

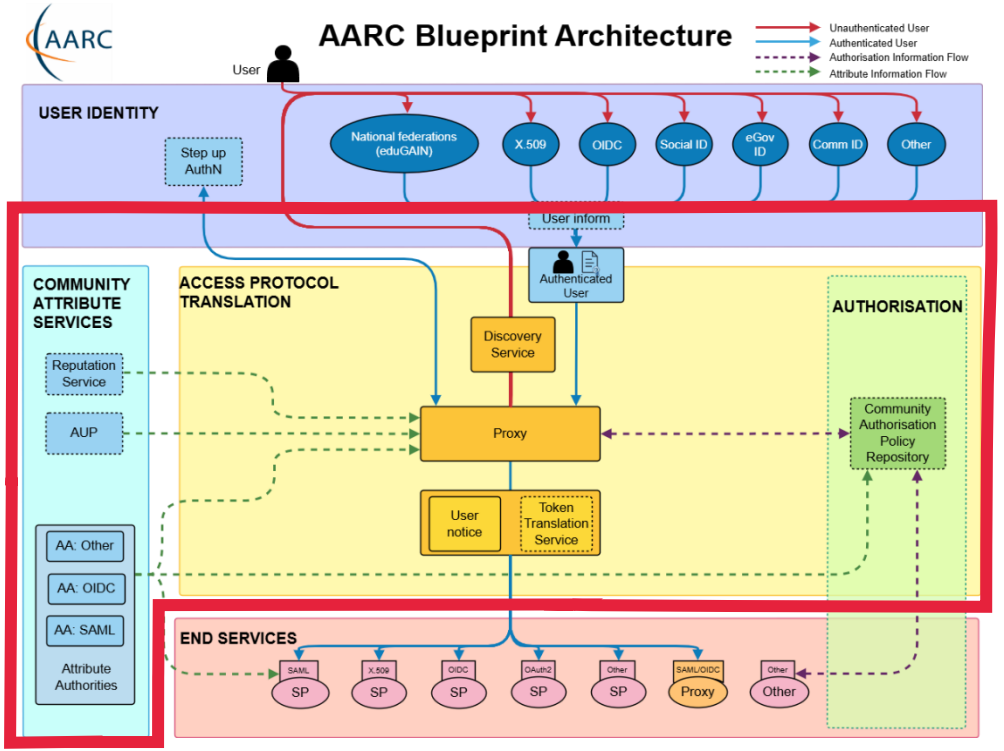
Adding a layer in the architecture for research collaboration

Bridging collaboration and authorisation layer
to identity federation

Authentication
(academic, or govID, or ...)

Network layer(s)

AARC Blueprint – making the bridge a first-class citizen



AARC BPA 2019 'Community First'
https://aarc-community.org/guidelines/aarc-g045/

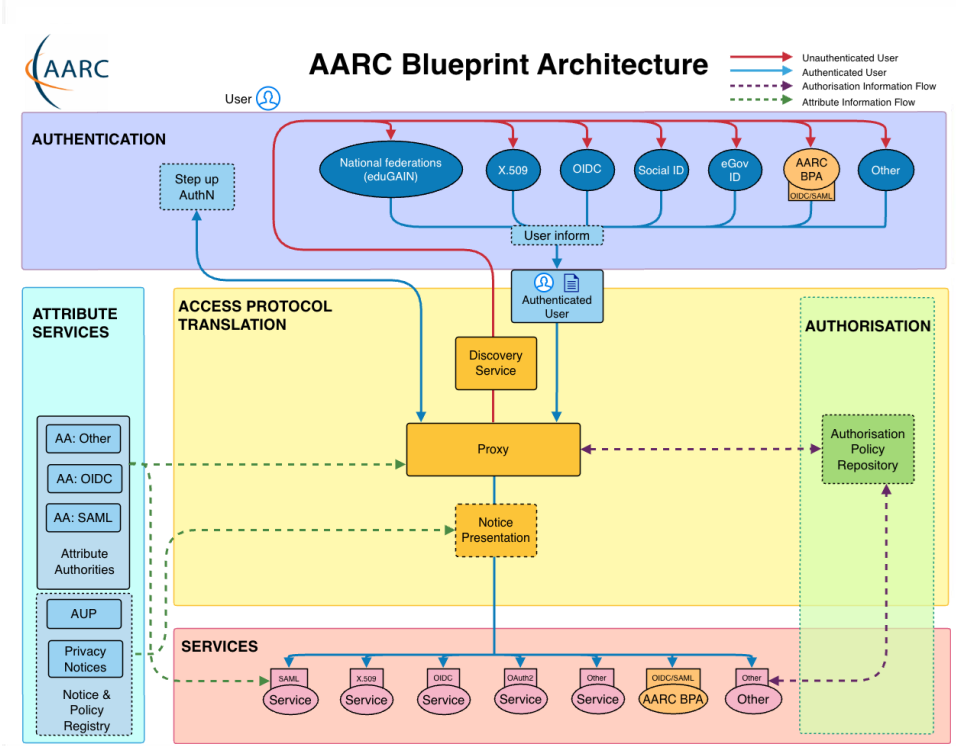
Facilitating the bridges

with interoperable **building blocks for 'AAI infrastructure' architects**

that are

- technology-agnostic
- have multiple implementations
- come with policy templates & good practice guides ☺

More than just nice colours



Not sure how to begin with the AARC Blueprint Architecture? There are plenty of guidelines available but it can be a minefield at first. You probably want to start by designing the high level approach of your infrastructure based on the AARC Blueprint Architecture. There are several general topics you should consider, such as Data Protection (AARC-G042) and Federated Security Incident Response (AARC-I051). Here you can find common questions matched to the relevant Blueprint Architecture component, along with links to guidelines that can help.

Community Attribute Services:

- How should attributes from multiple sources be aggregated? AARC-G003
- How should I express the home institute of a user? AARC-G025
- How should I express the identifier of a user AARC-G026
- What are the best practices for running my Attribute Authorities securely? AARC-G071
- Which Acceptable Use Policy should I use to facilitate interoperability? AARC-I044
- How should I infer the affiliation of a user? AARC-G057

Authorisation:

- How should I manage authorisation information from multiple sources? AARC-G006
- How should group and role information be expressed to facilitate interoperability? AARC-G002
- How should resource capabilities be expressed? AARC-G027

End Services:

- My service needs to act on behalf of the user – how should I handle credential delegation and impersonation? AARC-G005
- My services are not web based, how can I use identities from the proxy? AARC-G007
- How should Services hint which IdP they would like users to use? AARC-G049
- Which Security practices should I follow? AARC-G014

User Identity:

- How should I integrate Social Media Identity Providers? AARC-G008
- How should users link accounts, and how does that affect Assurance? AARC-G009
- How should services indicate that they would like users to authenticate with multifactor authentication, and how should my proxy forward that information? AARC-G029

Assurance:

- How should assurance information of external identities be calculated? AARC-G031
- What can I say about assurance of identities from social media accounts? AARC-G041
- How is assurance impacted by account linking? AARC-G009
- How should assurance information be shared with other infrastructures? AARC-G021
- Which Assurance Profiles should I use, there are so many! AARC-I050

Access Protocol Translation:

- Which best practices should I follow for my Token Translation Services? AARC-G004
- How should I translate from Identity Federation information to X.509 certificates? AARC-G010

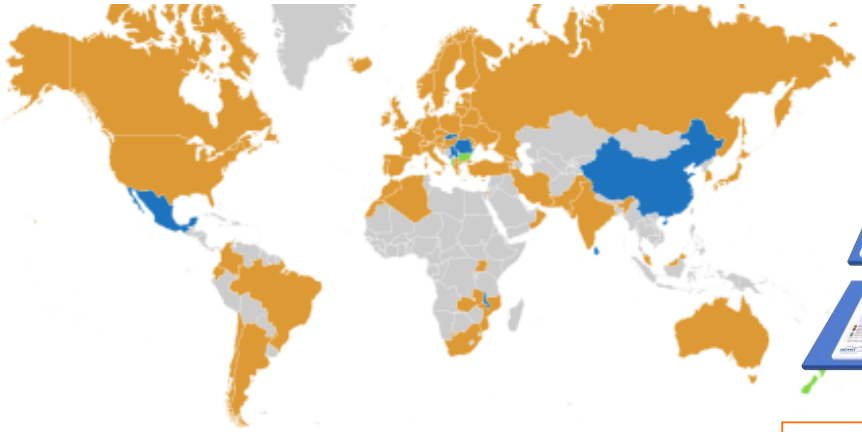
Proxies:

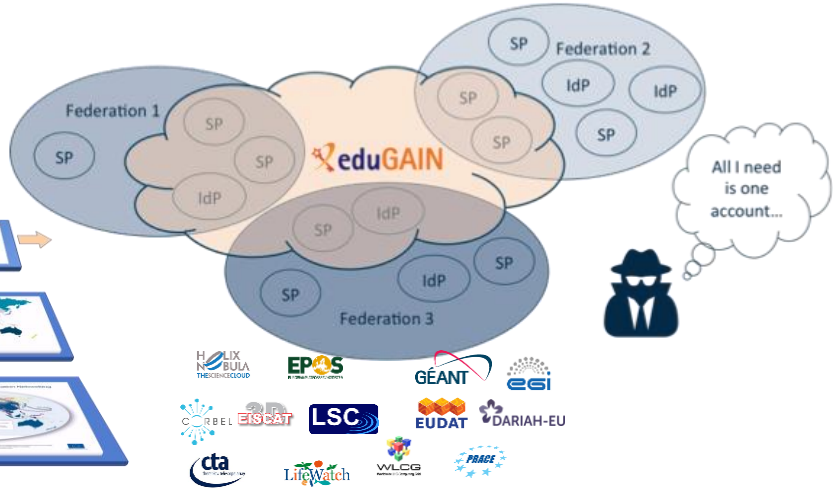
- How can I ensure that my proxy is able to accurately claim that it supports best practices in Identity Federation? AARC-G015
- How should I express the home institute of a user? AARC-G025
- How should I express the identifier of a user AARC-G026
- How should I express assurance information for users when interacting with another proxy? AARC-G021
- How can my proxy simplify the discovery process for end-users? AARC-G061
- How can my proxy route the user to the correct discovery service? AARC-G062

What next? Are you looking for a kick start with your policies? Take a look at the Policy Development Toolkit which provides a set of templates.

https://aarc-community.org/guidelines/

Now *what* have we built?!



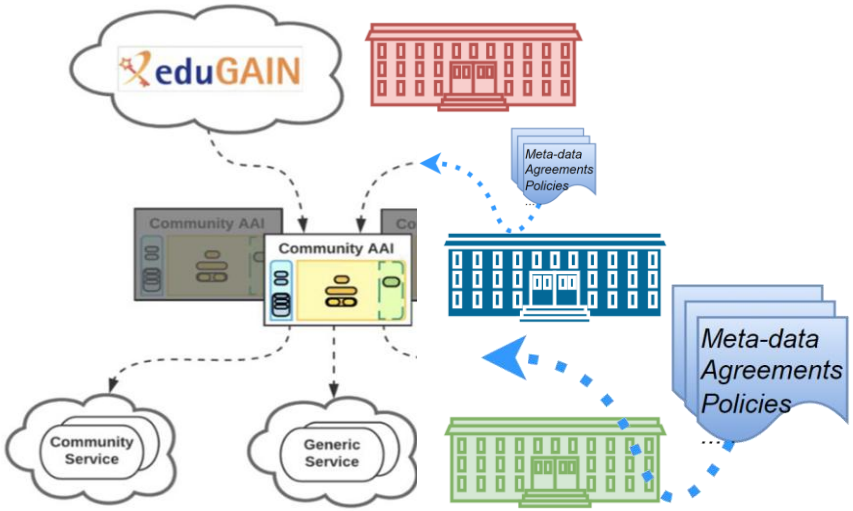


full of valuable resources
(data, network, services)

We have federation and single sign-on …
… but can we share security information when needed?
… timely and confidentially, protecting everyone's reputation?

left: eduGAIN interfederation extent in 2020; logos on the right from the European e-Infrastructures and ESFRIs; center graphic: AARC collaboration

The need to ‘decorate’ the arrows with trust

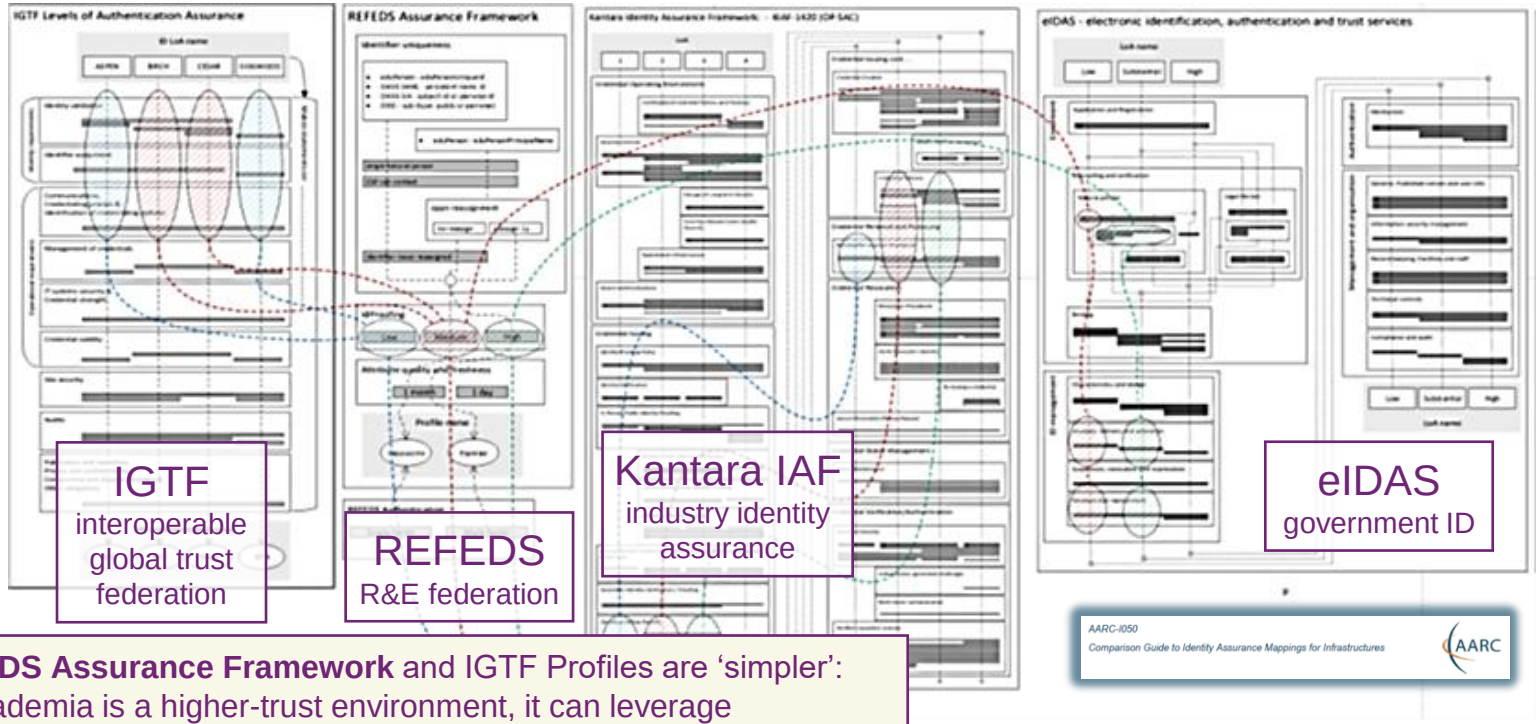


Each side of each arrow has *independent* parties

- we allow *them* to do part of the work *we* would otherwise do
- to make it easier and faster for users to perform their research
- but **we relinquish some control** beyond our organisation, our own policies, our own jurisdiction

***Why* would we trust them to do that?**

But even a simple *Who are you?* is not always simple …



IGTF
interoperable global trust federation

REFEDS
R&E federation

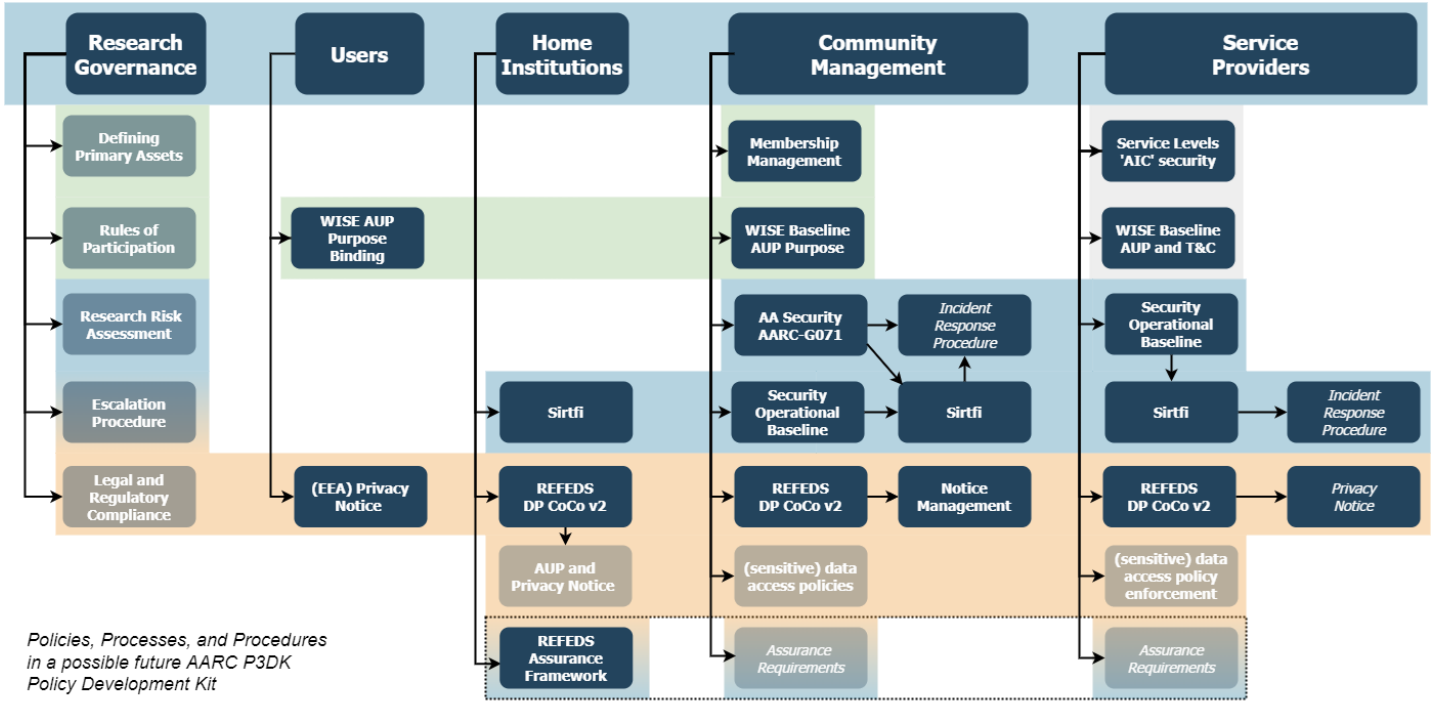
Kantara IAF
industry identity assurance

eIDAS
government ID

REFEDS Assurance Framework and IGTF Profiles are ‘simpler’: as academia is a higher-trust environment, it can leverage pre-established trust, self-assessment, and peer review

Source: https://aarc-community.org/guidelines/aarc-i050, Ian Neilson et al.
See **https://refeds.org/assurance** - join and interoperate on MFA+ and vetting

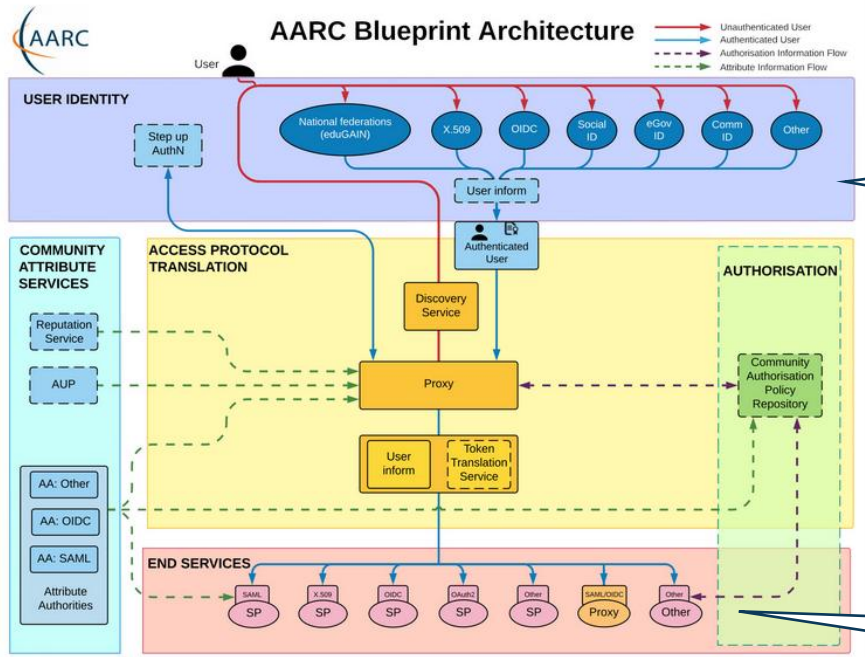
Building a *trust framework*: policy and procedural aspects of complex IT infrastructure



AARC-I082

https://aarc-community.org/guidelines/aarc-i082/

Practices we already have, practices we need to harmonise



Authentication and identity sources
- NIST SP800-63
- FIPS140
- ISO 27001
- IGTF AP Profiles
- REFEDS MFA
- REFEDS Assurance Framework

so … what about standards for the operation of this 'proxy' thing?

Service provider operations
- ISO27k
- NIS2
- ITSRM2

https://aarc-community.org/guidelines/aarc-g071/

 while for identity sources and for services there is extensive normalisation, our AARC BPA 'proxy' did not yet …

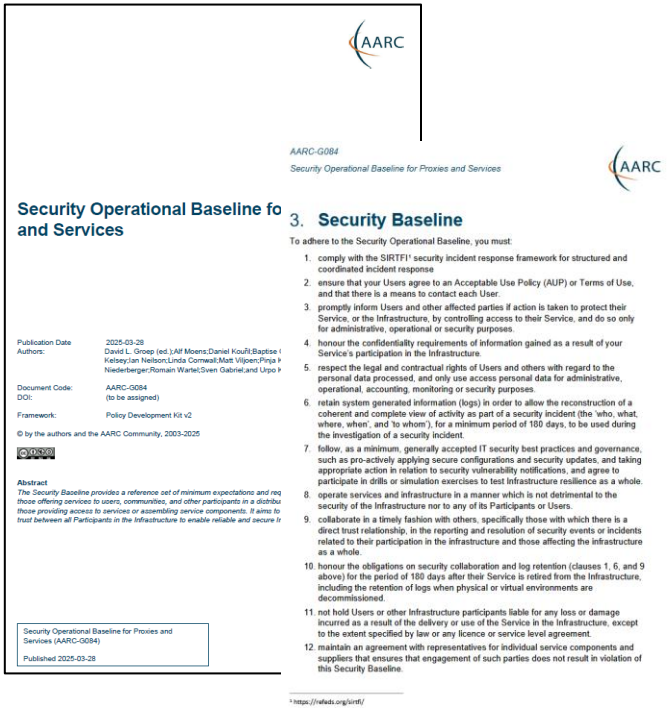
Information Security: Security Operational Baseline

Service Security Policy was re-used widely, in EGI, AARC, WLCG, but naturally diverged over time

- with national implementations and specialisations
- included in EOSC Interoperability Framework as '*Security Operational Baseline*'

So the new AARC PDK converges on a **common Baseline**

- included in the EOSC AAI WG Federation 2025 requirements
- with guidance and FAQ



AARC-G084

Security Operational Baseline for Proxies and Services

Security Operational Baseline fo
and Services

Publication Date: 2025-03-28
Authors: David L. Groep (ed.);Alf Moens;Daniel Kouřil;Baptiste
Kelsey;Jan Neilson;Linda Cornwall;Matt Viljoen;Pinja
Niederberger;Romain Wartel;Sven Gabriel;and Urpo

Document Code: AARC-G084
DOI: (to be assigned)

Framework: Policy Development Kit v2

Abstract
*The Security Baseline provides a reference set of minimum expectations and req
those offering services to users, communities, and other participants in a distribu
those providing access to services or assembling service components. It aims to
trust between all Participants in the Infrastructure to enable reliable and secure I*

Security Operational Baseline for Proxies and Services (AARC-G084)

Published 2025-03-28

3. Security Baseline

To adhere to the Security Operational Baseline, you must:

1. comply with the SIRTFI[1] security incident response framework for structured and coordinated incident response
2. ensure that your Users agree to an Acceptable Use Policy (AUP) or Terms of Use, and that there is a means to contact each User.
3. promptly inform Users and other affected parties if action is taken to protect their Service, or the Infrastructure, by controlling access to their Service, and do so only for administrative, operational or security purposes.
4. honour the confidentiality requirements of information gained as a result of your Service's participation in the Infrastructure.
5. respect the legal and contractual rights of Users and others with regard to the personal data processed, and only use access personal data for administrative, operational, accounting, monitoring or security purposes.
6. retain system generated information (logs) in order to allow the reconstruction of a coherent and complete view of activity as part of a security incident (the 'who, what, where, when', and 'to whom'), for a minimum period of 180 days, to be used during the investigation of a security incident.
7. follow, as a minimum, generally accepted IT security best practices and governance, such as pro-actively applying secure configurations and security updates, and taking appropriate action in relation to security vulnerability notifications, and agree to participate in drills or simulation exercises to test Infrastructure resilience as a whole.
8. operate services and infrastructure in a manner which is not detrimental to the security of the Infrastructure nor to any of its Participants or Users.
9. collaborate in a timely fashion with others, specifically those with which there is a direct trust relationship, in the reporting and resolution of security events or incidents related to their participation in the infrastructure and those affecting the infrastructure as a whole.
10. honour the obligations on security collaboration and log retention (clauses 1, 6, and 9 above) for the period of 180 days after their Service is retired from the Infrastructure, including the retention of logs when physical or virtual environments are decommissioned.
11. not hold Users or other Infrastructure participants liable for any loss or damage incurred as a result of the delivery or use of the Service in the Infrastructure, except to the extent specified by law or any licence or service level agreement.
12. maintain an agreement with representatives for individual service components and suppliers that ensures that engagement of such parties does not result in violation of this Security Baseline.

[1] https://refeds.org/sirtfi

AARC-G084 https://doi.org/10.5281/zenodo.7396724

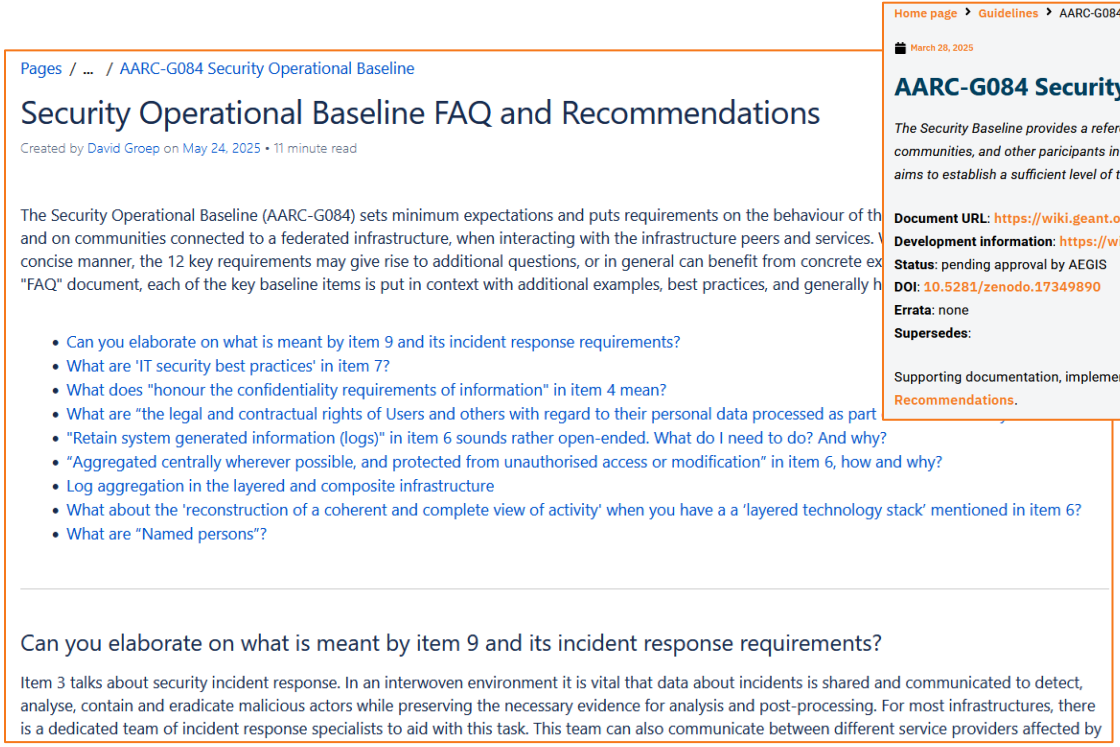
The 12 points of AARC-G084

AARC-G084

1. comply with the SIRTFI security incident response framework for structured and coordinated incident response [ref to SIRTFI]
2. ensure that your Users agree to an Acceptable Use Policy (AUP) or Terms of Use, and that there is a means to contact each User.
3. promptly inform Users and other affected parties if action is taken to protect their Service, or the Infrastructure, by controlling access to their Service, and do so only for administrative, operational or security purposes.
4. honour the confidentiality requirements of information gained as a result of your Service's participation in the Infrastructure.
5. respect the legal and contractual rights of Users and others with regard to the personal data processed, and only use access personal data for administrative, operational, accounting, monitoring or security purposes.
6. retain system generated information (logs) in order to allow the reconstruction of a coherent and complete view of activity as part of a security incident (the 'who, what, where, when', and 'to whom'), for a minimum period of 180 days, to be used during the investigation of a security incident.
7. follow, as a minimum, generally accepted IT security best practices and governance, such as pro-actively applying secure configurations and security updates, and taking appropriate action in relation to security vulnerability notifications, and agree to participate in drills or simulation exercises to test Infrastructure resilience as a whole.
8. operate services and infrastructure in a manner which is not detrimental to the security of the Infrastructure nor to any of its Participants or Users.
9. collaborate in a timely fashion with others, specifically those with which there is a direct trust relationship, in the reporting and resolution of security events or incidents related to their participation in the infrastructure and those affecting the infrastructure as a whole.
10. honour the obligations on security collaboration and log retention (clauses 1, 6, and 9 above) for the period of 180 days after their Service is retired from the Infrastructure, including the retention of logs when physical or virtual environments are decommissioned.
11. not hold Users or other Infrastructure participants liable for any loss or damage incurred as a result of the delivery or use of the Service in the Infrastructure, except to the extent specified by law or any licence or service level agreement.
12. maintain an agreement with representatives for individual service components and suppliers that ensures that engagement of such parties does not result in violation of this Security Baseline

FAQ and implementation guidance

AARC-G084



Pages / ... / AARC-G084 Security Operational Baseline

Security Operational Baseline FAQ and Recommendations

Created by David Groep on May 24, 2025 • 11 minute read

The Security Operational Baseline (AARC-G084) sets minimum expectations and puts requirements on the behaviour of th
and on communities connected to a federated infrastructure, when interacting with the infrastructure peers and services. V
concise manner, the 12 key requirements may give rise to additional questions, or in general can benefit from concrete ex
"FAQ" document, each of the key baseline items is put in context with additional examples, best practices, and generally h

- Can you elaborate on what is meant by item 9 and its incident response requirements?
- What are 'IT security best practices' in item 7?
- What does "honour the confidentiality requirements of information" in item 4 mean?
- What are "the legal and contractual rights of Users and others with regard to their personal data processed as part
- "Retain system generated information (logs)" in item 6 sounds rather open-ended. What do I need to do? And why?
- "Aggregated centrally wherever possible, and protected from unauthorised access or modification" in item 6, how and why?
- Log aggregation in the layered and composite infrastructure
- What about the 'reconstruction of a coherent and complete view of activity' when you have a a 'layered technology stack' mentioned in item 6?
- What are "Named persons"?

Can you elaborate on what is meant by item 9 and its incident response requirements?

Item 3 talks about security incident response. In an interwoven environment it is vital that data about incidents is shared and communicated to detect, analyse, contain and eradicate malicious actors while preserving the necessary evidence for analysis and post-processing. For most infrastructures, there is a dedicated team of incident response specialists to aid with this task. This team can also communicate between different service providers affected by

Home page › Guidelines › AARC-G084

March 28, 2025

AARC-G084 Security Operational Baseline

The Security Baseline provides a reference set of minimum expectations and requirements of the behaviour of those offering services to users, communities, and other paricipants in a distributed proxy ecosystem, and of those providing access to services or assembling service components. It aims to establish a sufficient level of trust between all Participants in the Infrastructure to enable reliable and secure Infrastructure operation.

Document URL: https://wiki.geant.org/download/attachments/999948380/AARC-G084-Security-Operational-Baseline-PDKv2.pdf
Development information: https://wiki.geant.org/spaces/AARC/pages/999948380/AARC-G084+Security+Operational+Baseline
Status: pending approval by AEGIS
DOI: 10.5281/zenodo.17349890
Errata: none
Supersedes:

Supporting documentation, implementation suggestions and background information is available in the Security Operational Baseline FAQ and Recommendations.

WISE AUP: actionable policy across infrastructures

Acceptable Use Policy and Conditions of Use

This Acceptable Use Policy and Conditions of Use ("AUP") defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and services ("Services") as granted by {community, agency, or infrastructure name} for the purpose of {describe the stated goals and policies governing the intended use}.

<To further define and limit what constitutes acceptable use, the community, agency, or infrastructure may optionally add additional information, rules or conditions, or references thereto, here or at the placeholder below. These additions must not conflict with the clauses 1-10 below, whose wording and numbering must not be changed.>

1. You shall only use the Services in a manner consistent with the purposes and limitations described above; you shall show consideration towards other users including by not causing harm to the Services; you have an obligation to collaborate in the resolution of issues arising from your use of the Services.
2. You shall only use the Services for lawful purposes and not breach, attempt to breach, nor circumvent administrative or security controls.
3. You shall respect intellectual property and confidentiality agreements.
4. You shall protect your access credentials (e.g. passwords, private keys or multi-factor tokens); no intentional sharing is permitted.
5. You shall keep your registered information correct and up to date.
6. You shall promptly report known or suspected security breaches, credential compromise, or misuse to the security contact stated below; and report any compromised credentials to the relevant issuing authorities.
7. Reliance on the Services shall only be to the extent specified by any applicable service level agreements listed below. Use without such agreements is at your own risk.
8. Your personal data will be processed in accordance with the privacy statements referenced below.
9. Your use of the Services may be restricted or suspended, for administrative, operational, or security reasons, without prior notice and without compensation.
10. If you violate these rules, you may be liable for the consequences, which may include your account being suspended and a report being made to your home organisation or to law enforcement.

<Insert additional numbered clauses here>

The administrative contact for this AUP is:
{email address for the community, agency, or infrastructure name}
The security contact for this AUP is:
{email address for the community, agency, or infrastructure security contact}
The privacy statements (e.g. Privacy Notices) are located at: {URL}
Applicable service level agreements are located at: <URLs>

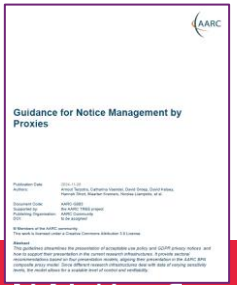
Purpose binding
ensure use is as intended for access grant

Terms and Conditions
research data access conditions, permits, grant conditions

WISE Baseline AUP
common 10 commandments that allow seamless cross-sectoral user movement

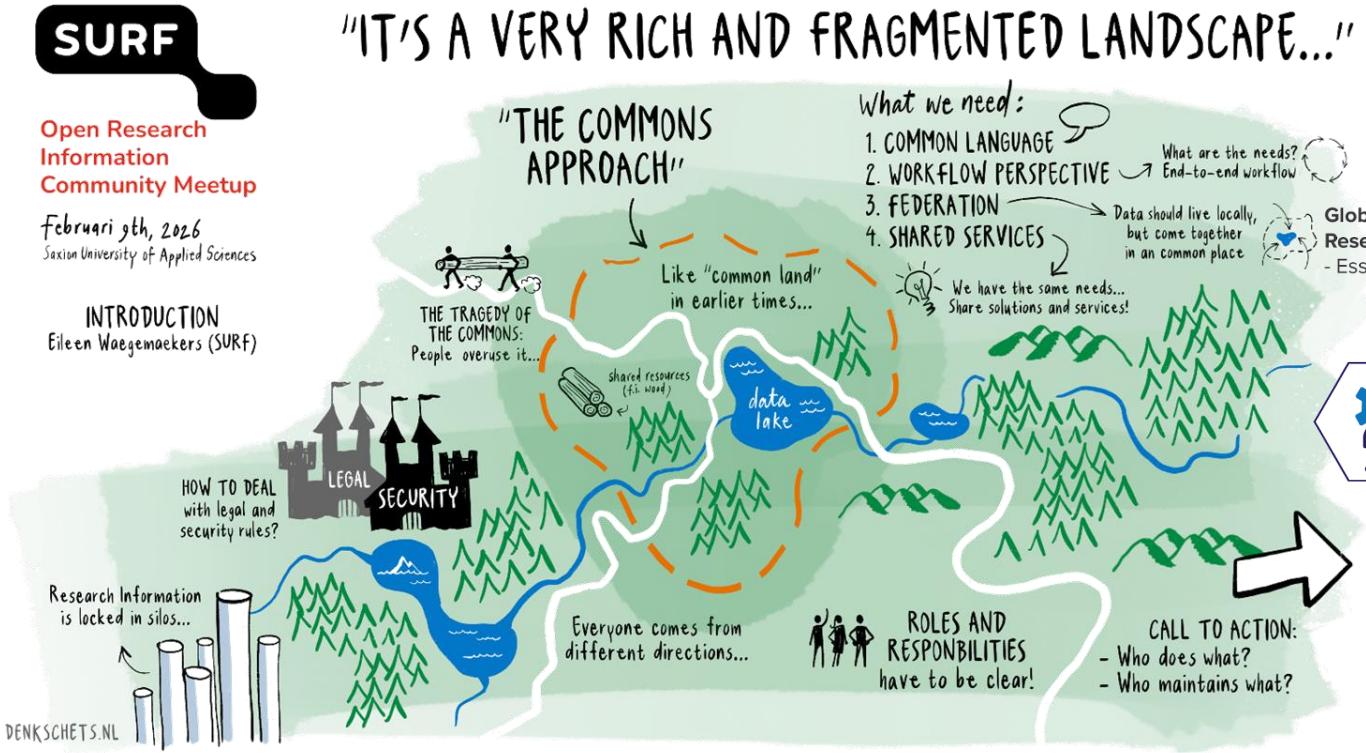
Service level agreements
promises and recourse

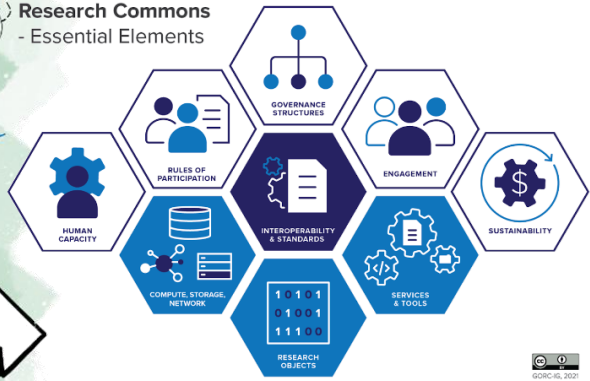
Privacy notice references
for *access* personal data policies



https://wise-community.org/wise-baseline-aup/

Since be it research information, research cloud, or open science …





Thanks to Eileen Waegemaekers, Maarten Hoogerwerf, image by *denkschets.nl* during an ORI event. Right: RDA GORC-WG, https://www.rd-alliance.org/groups/gorc-international-model-wg/

Infrastructure as a composite set of connected services

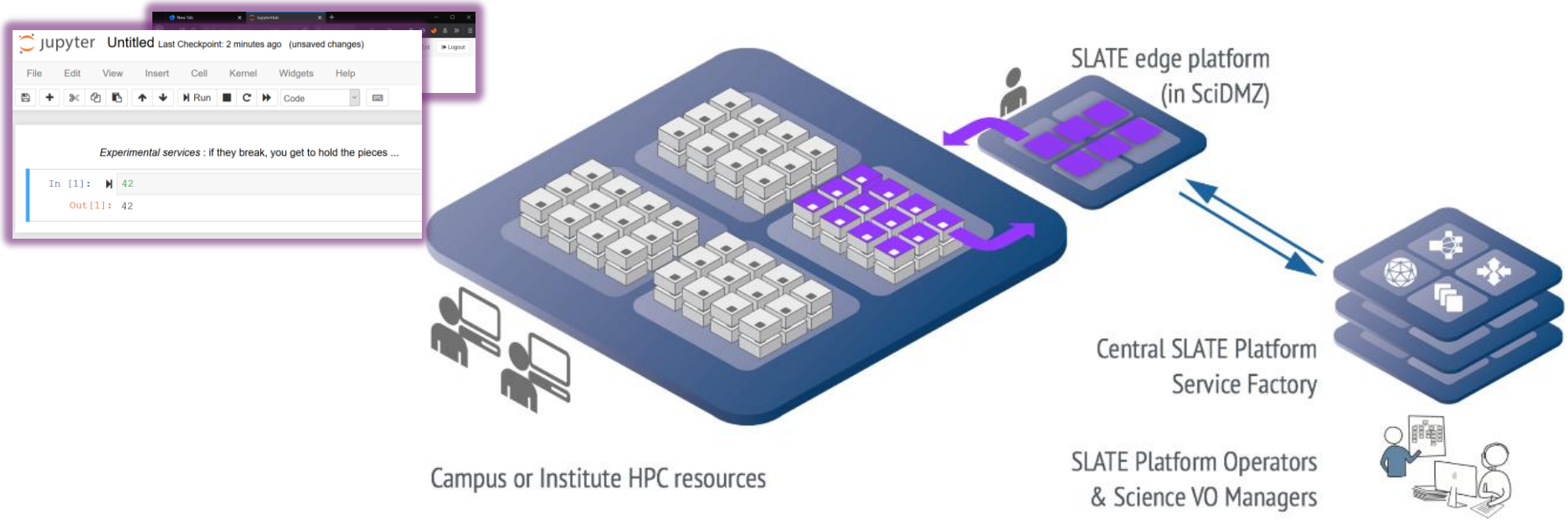
IT Service Management (ISO20000, ITIL, FitSM) promote
a *specific definition* of service portfolio management:

> "**Product/service portfolio** The product/service portfolio is the complete set of products and/or services ***that are managed by the organization***, and it represents the organization's commitments and investments across all its customers and market spaces. …" [ITIL v4, chapter 5]

Concept of 'services' in collaborative research is quite different:

- coming from existing collaborations and infrastructures, many or most services *already pre-exists and used extensively* by research and collaborative administration;
- these 'outsiders' are an *essential aspects*: they should be embraced, as they support the primary mission of the organization (e.g. research & education);
- whether a 'service' is operated by a third party, or outside our local ITSM control, is *immaterial to the value of the service*

Example: an overlay network of containers …



‘alien containers’ HPC integration - container computing, using curated application images

Image sources: NDPF JupyterHub service “Callysto”; SLATE: Service Layer At The Edge – Rob Gartner (UChicago), Shawn KcMee (UMich) *et al.* – slateci.io

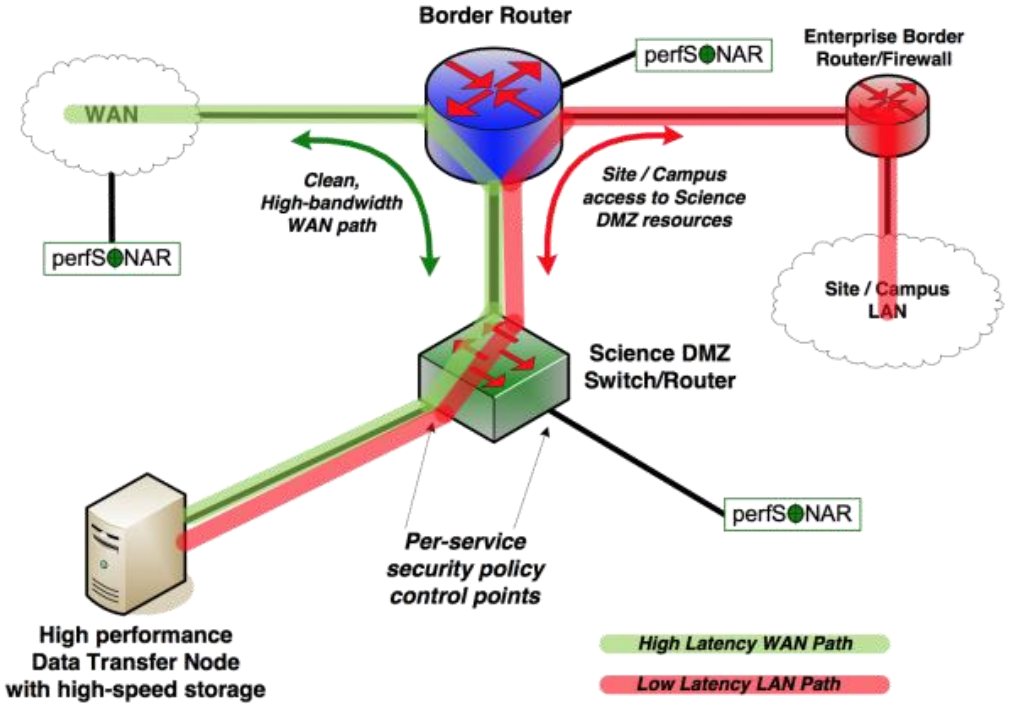
‘ScienceDMZ’

Accessible from the outside world
with predicable performance
and data access for research

‘where research services, data, and researchers meet’

latency hiding through caching

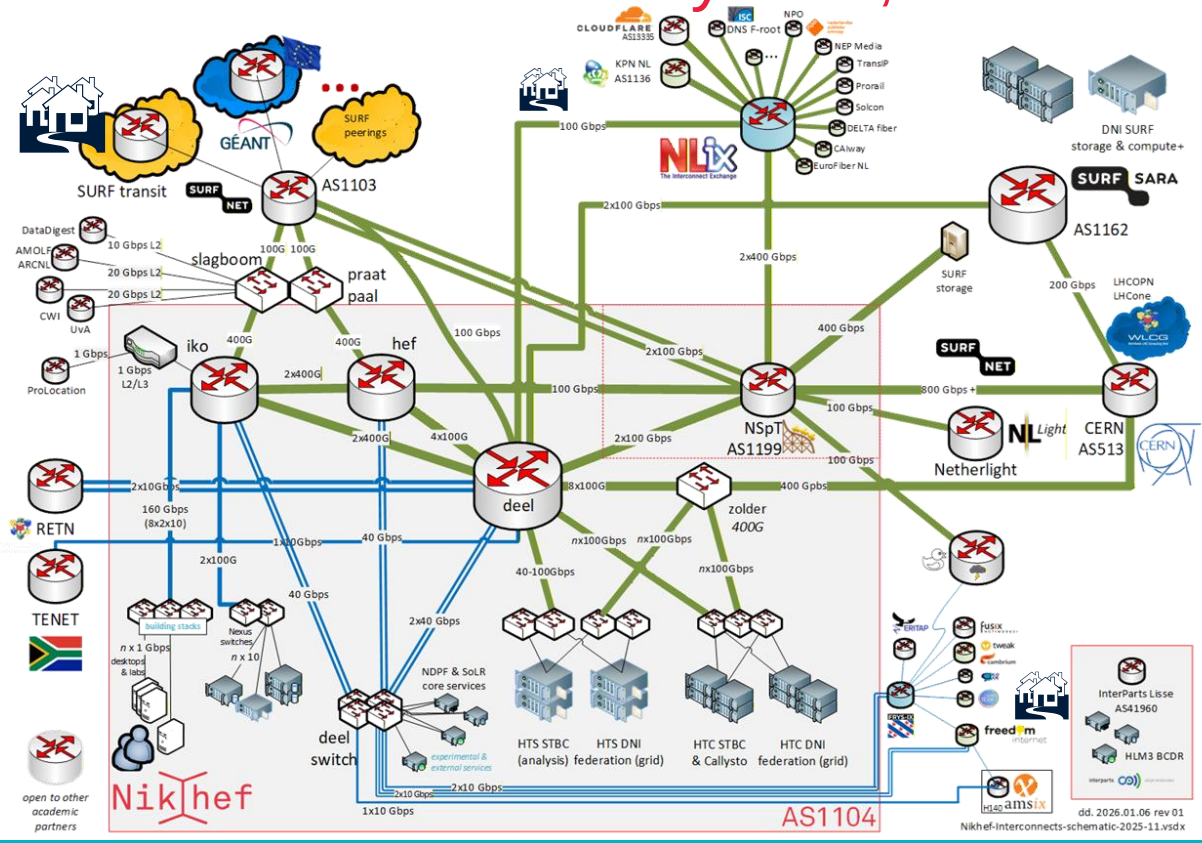
security zoning/segmentation
protects specific data sets



outside any ‘enterprise’ perimeter since *any* stateful device will be disruptive

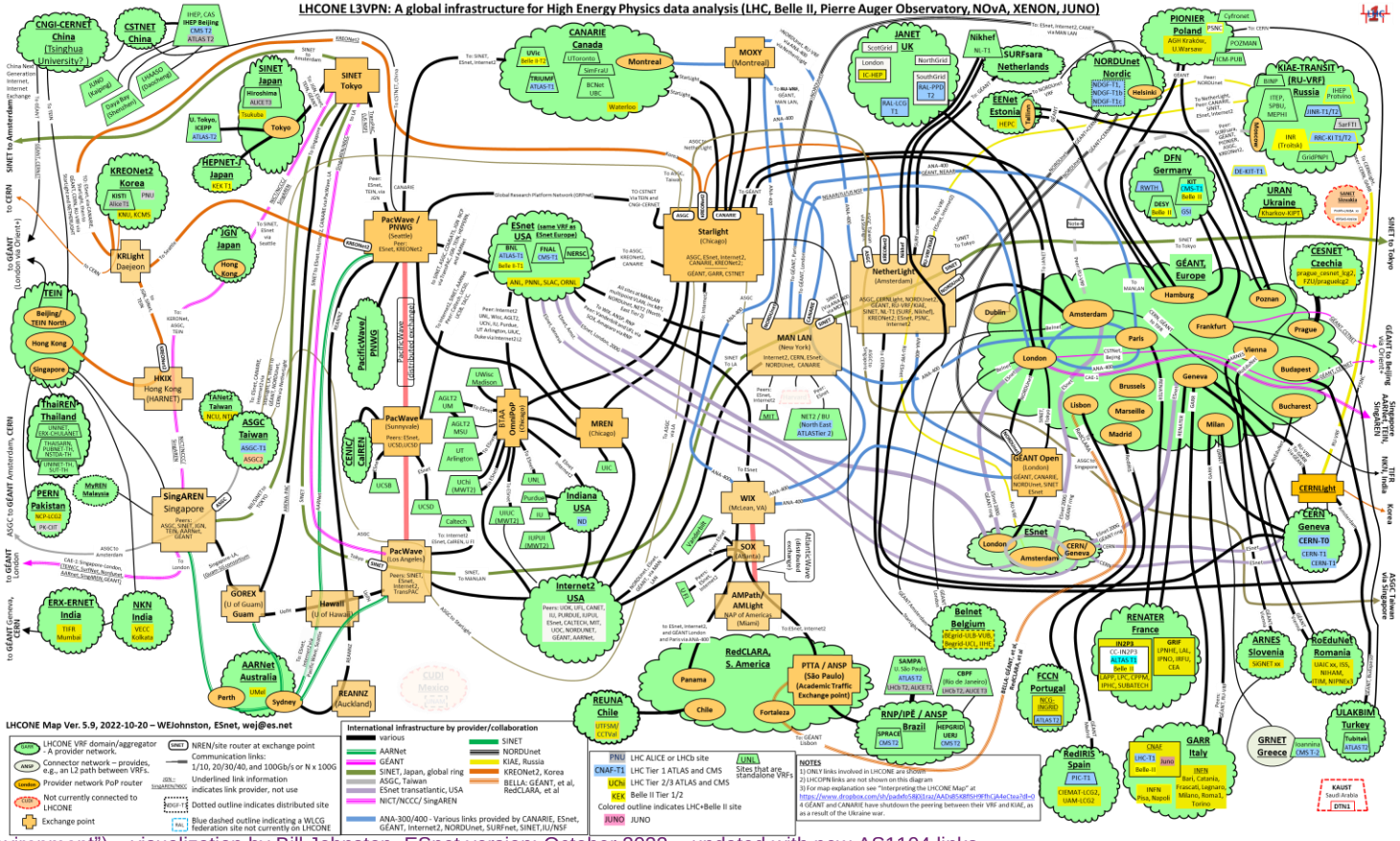
Image and ‘ScienceDMZ’ concept promulgated by ESnet (see fasterdata.es.net) – image: Eli Dart

Just one random autonomous system, AS1104



AS1104 state as of Oct 2024

LHCone



LHCone ("LHC Open Network Environment") – visualization by Bill Johnston, ESnet version: October 2022 – updated with new AS1104 links

Exercising the network, for sensor data and events

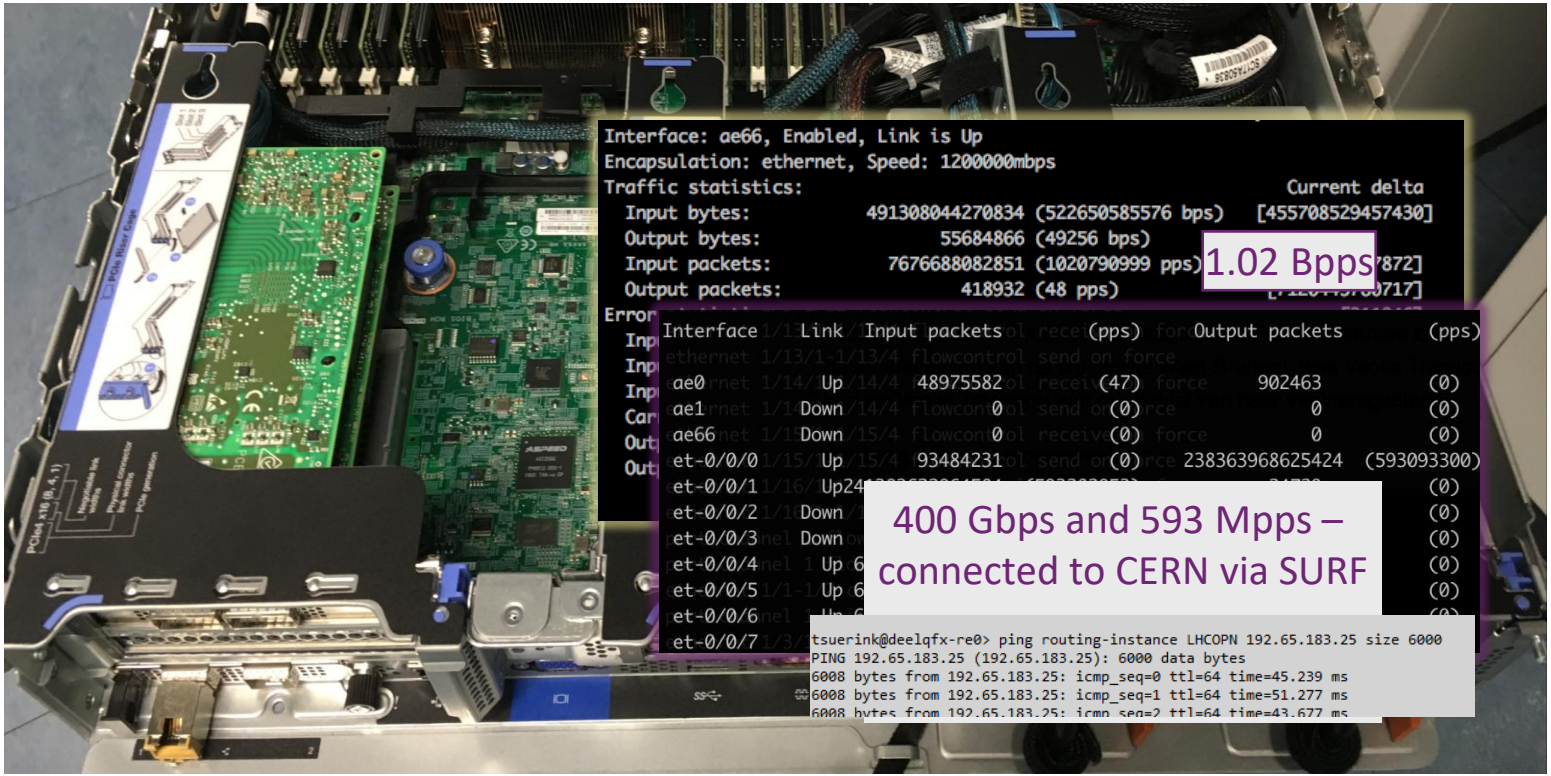
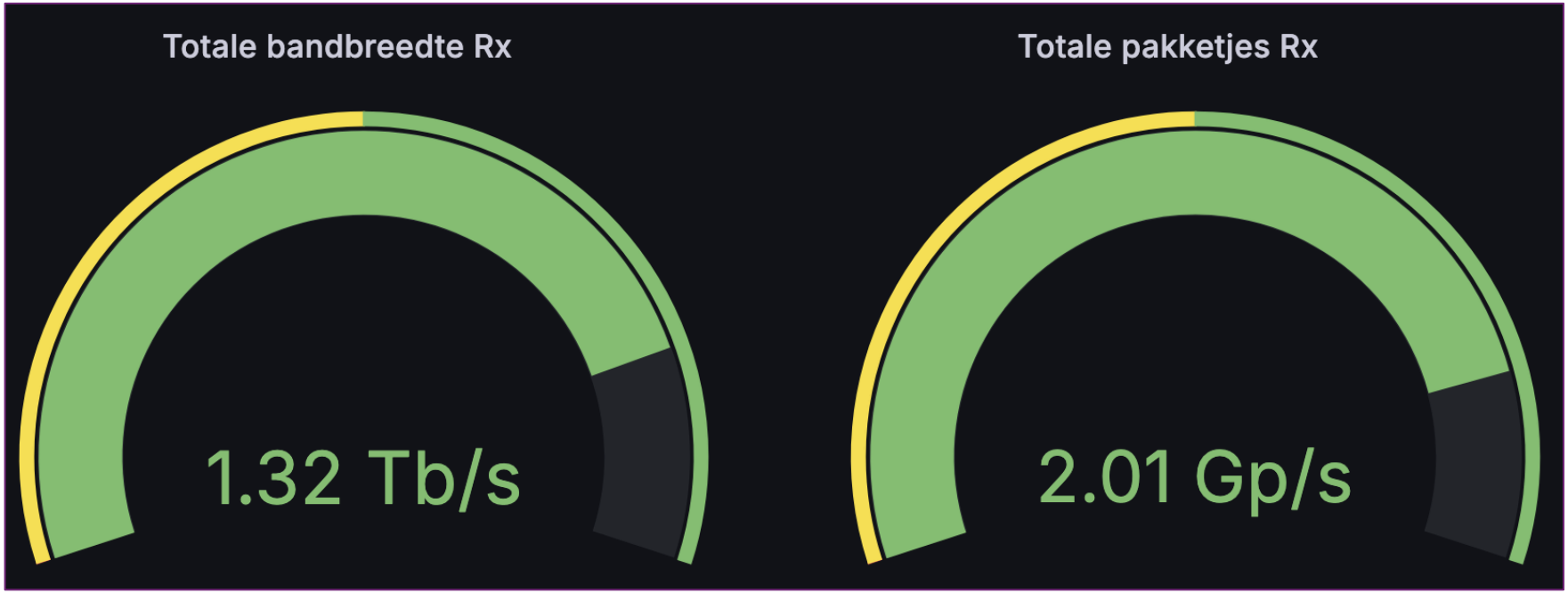


Image: ballenbak.nikhef.nl, Tristan Suerink, 2022

with packets being more destructive than bandwidth …



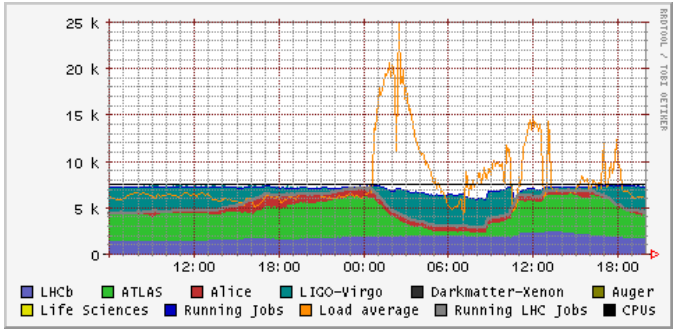
https://wiki.nikhef.nl/grid/2Bpps_Machine - in preparation for the 2025 National ‘Resilience Exercise’

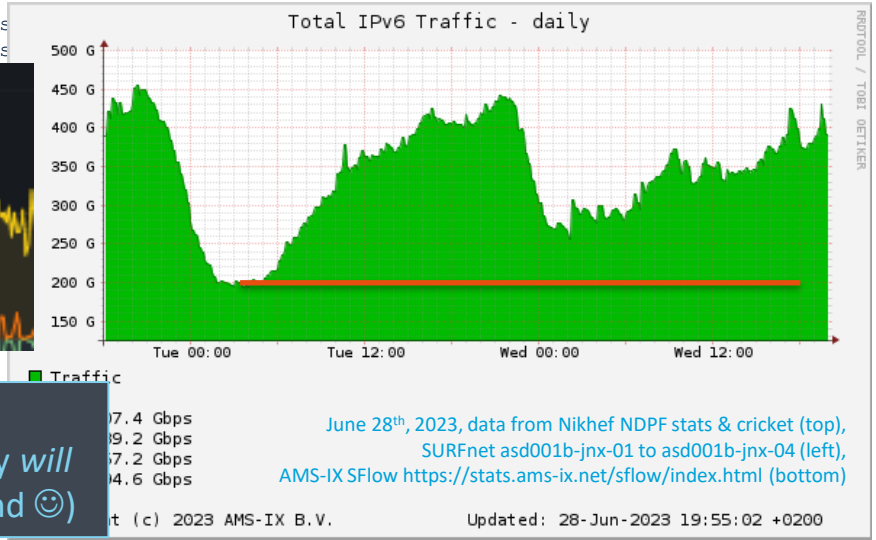
And some traffic is triggered by researchers scaling up ‘accidentally’ from a laptop to a cluster without too much thought

A researcher doing mass creation of containers, rebuilding their python ‘virtual env’ for each job, running on >> 4000 cores

```
[root@wn-pep-002 ~]# top
top - 09:40:47 up 71 days, 12:17,  2 users,  load average: 110.38, 101.43, 106.3
Tasks: 700 total,   7 running, 666 sleeping,   0 stopped,  27 zombie
%Cpu(s): 17.0 us,  2.0 sy,  0.0 ni, 81.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem : 39462902+total, 23514457+free, 10406320 used, 14907812+buff/cache
KiB Swap: 67108860 total, 66841340 free,   267520 used. 37964784+avail Mem

   PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
 82661 ligo000   20   0 5618756 396356    924 R 360.0  0.1   5:14.43 mksquashfs
 72615 ligo000   20   0 5626336 248516    816 R  90.0  0.1   5:44.11 mksquashfs
 83257 ligo000   20   0 5611608 219300    852 S  90.0  0.1   1:1
 ...
```





Pulling the python packages at line rate and downloading public python repositories ultimately *will* flood SURFnet (though neither CloudFlare or I mind ☺)

June 28th, 2023, data from Nikhef NDPF stats & cricket (top), SURFnet asd001b-jnx-01 to asd001b-jnx-04 (left), AMS-IX SFlow https://stats.ams-ix.net/sflow/index.html (bottom)

Research data traffic looks like … a DDoS to others ☺

Belastingdienst

Home ≡ Menu Zoeken

Home > Actueel > ICT en informatievoorziening > De systemen testen dankzij een unieke samenwerking

Lees voor

De systemen testen dankzij een unieke samenwerking

Op dez
Een goe
Examer
Wat geb
Vragen
Terug n

Het begon in 2018. Een bijzondere samenwerking tussen overheden, internetproviders- en exchanges, academische instanties, non-
pr
du
sin
n plat
vapen
alitie.

Dinsdag 14 maart 2023 | Het laatste nieuws het eerst op NU.nl

Door Rutger Otto

12 feb 2023 om 05:02
Update: een maand geleden

202 reacties

Betastingsdienst

Home

Home > Aanslagen > Ik heb een DDoS aanslag ontvangen - wat nu?

Ik heb een DDoS aanslag op mijn netwerk ontvangen - wat nu?

U ontvangt een DDoS aanslag op uw netwerk, bijvoorbeeld omdat u vergeten bent werkende tegenmaatregelen te nemen. Er staat dan een geschat aantal pakketten per seconde op uw monitoring.

Een goed begin

De voorbereidingen van de avond beginnen ver voordat de oefening gepland staat. Elke organisatie bepaalt welke systemen ze willen aanvallen en hoe de aanval uitgevoerd wordt. Het 'red team' is verantwoordelijk voor de aanvallen, het 'blue team' voor de verdediging. Eén van de partijen die avond is Nikhef. Tristan, IT architect bij Nikhef, geeft aan dat zij dit belangeloos doen, gedreven door een maatschappelijke motivatie.

Nikhef is het Nationaal instituut voor subatomaire fysica in Nederland. Het beschikt over een gigantische bandbreedte, wat noodzakelijk is voor een dergelijke oefening waarbij zeer veel data wordt verstuurd. Zij zijn onderdeel van de aanvallende teams en

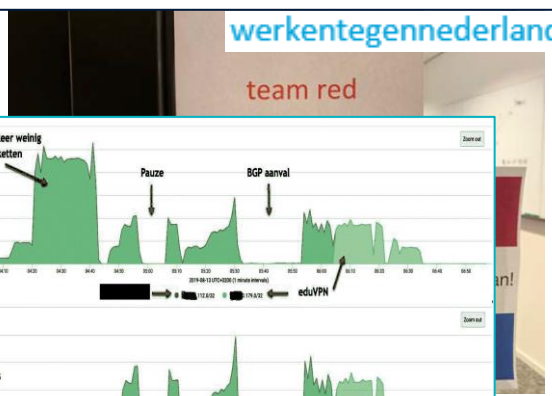
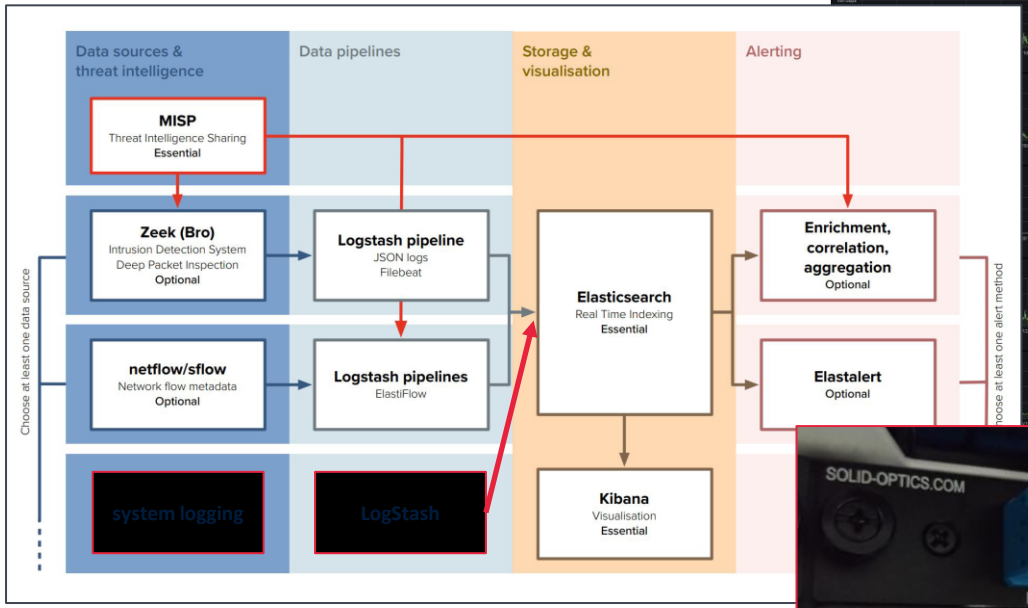
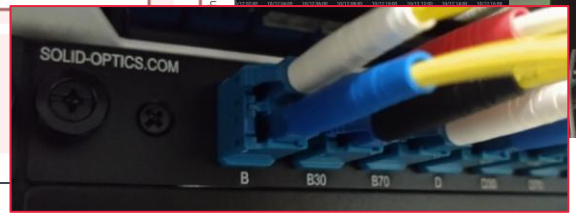


Image sources: belastingdienst.nl, rws.nl, nu.nl

‘open’ does not mean ‘insecure’





650 GByte/day ingest; 400Gbps+ monitoring through optical taps and mirroring; MISP intel from CERN, SURF, and private intel sources

Nikhef SOC design/management by Daniel Geerts, Sil Westerveld, Jouke Roorda.
WLCG SOC WG model: Liviu Valsan (CERN) and David Crooks (STFC RAL)

‘Sirtfi’ – what makes federated security different?

SIRTFI
Security Incident Response Trust Framework for Federated Identity

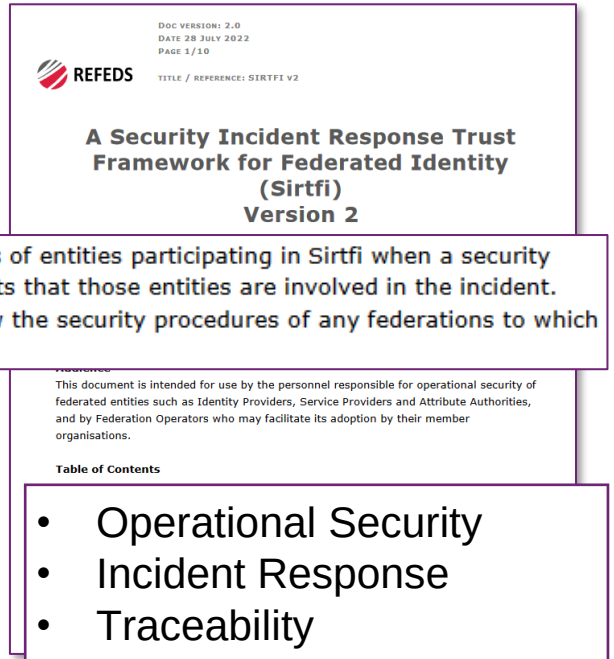
Organisations probably do ‘something reasonable’ for their own security ... but may not realise the **implications for others**

Sirtfi targets coordinated **response in a federated context**:

1. Enable **communication** and coordination in managing federated security incidents
2. Relevant **event data** is available to help collaborating incident responders
3. **Security protections are applied** to federated transactions

Clarifies security incident response by an IdP or SP, and **organisation can self-asserts** in federation meta-data

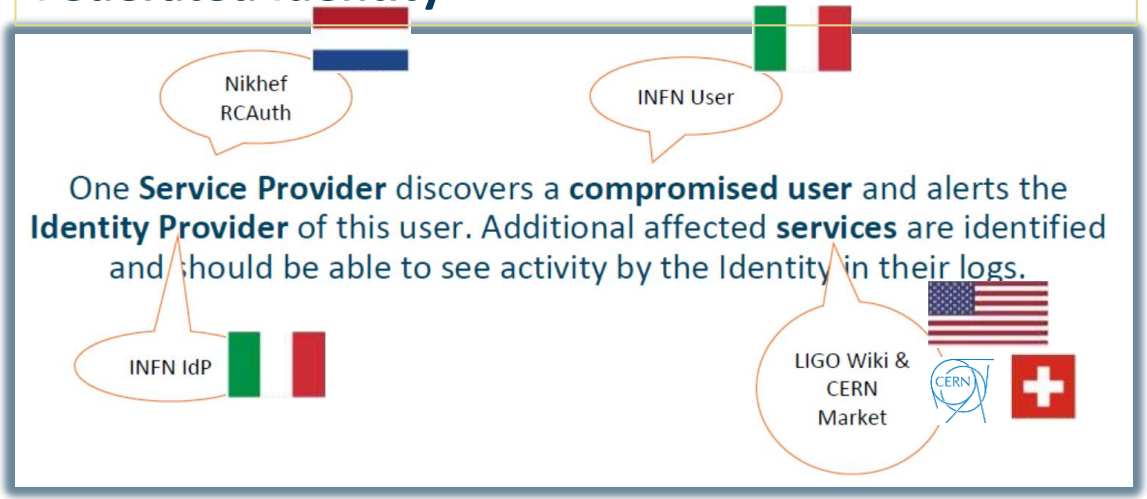
https://refeds.org/sirtfi

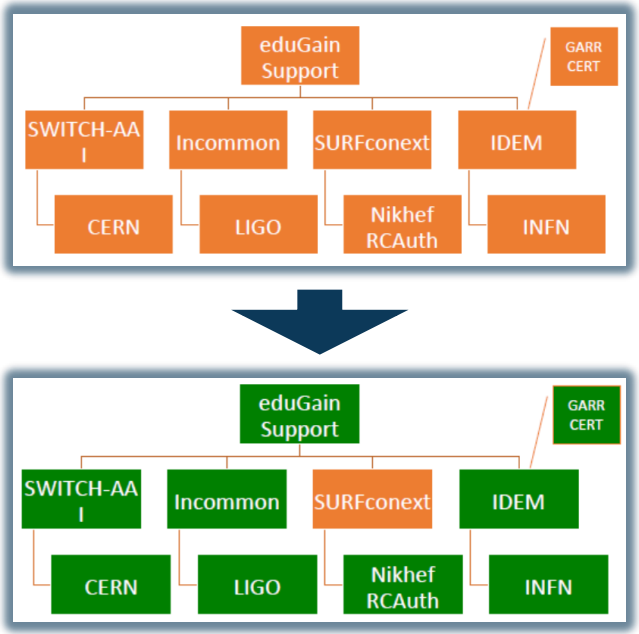


A federated community security challenge

Can we coordinate our collective R&E response?
'challenges' based on the *Sirtfi* contact model

Security Incident Response Trust Framework for Federated Identity

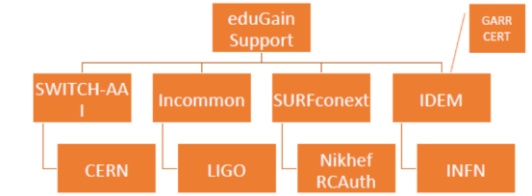




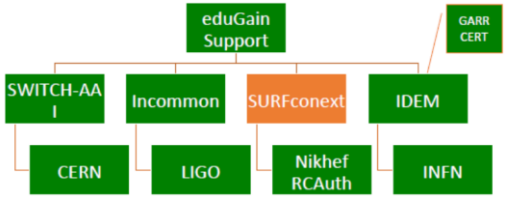
parties involved in response challenge

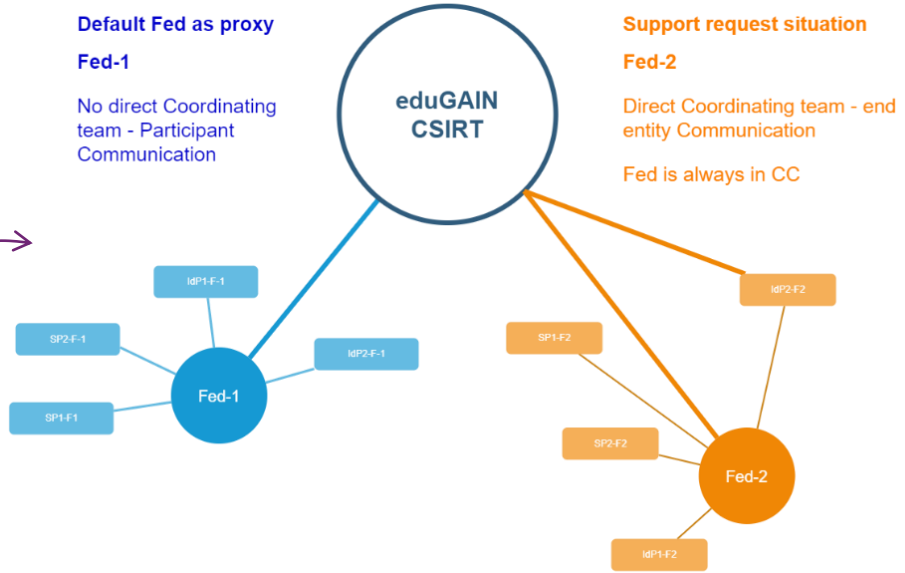
Report-outs see **https://wiki.geant.org/display/AARC/Sirtfi+Communications+Challenges%2C+AARC2-TNA3.1**

Response across IdP-SP Proxies: the limits of Sirtfi version 1



Srtfi v1

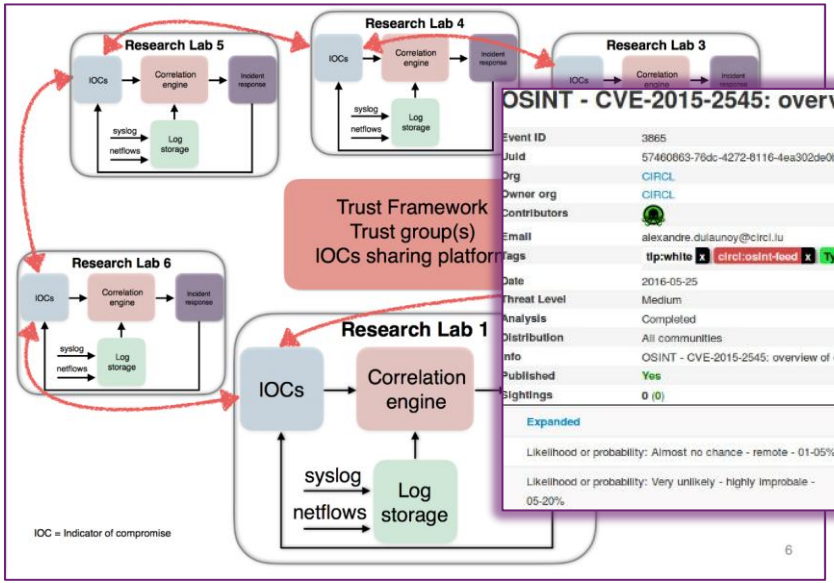




GÉANT | eduGAIN | CSIRT

joint work with GN5 EnCo and eduGAIN CSIRT

Sharing threat intel – working with our community

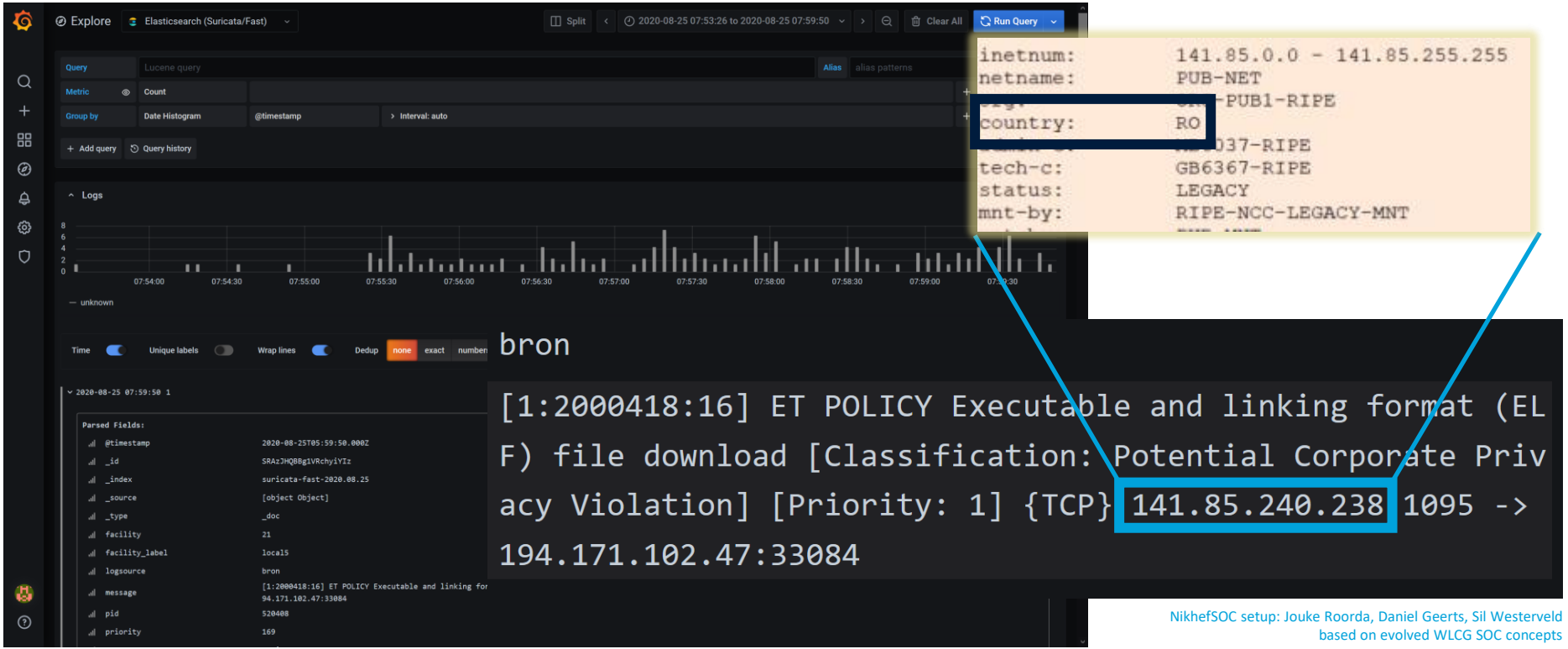


AARC I-051 Guide to federated incident response
https://aarc-community.org/guidelines/aarc-i051/

WLCG SOC WG, Research SOC (US), MISP by Circl.lu (https://www.circl.lu/services/misp-malware-information-sharing-platform/)

A single site sees only so much …

many ‘false warnings’ when industry-standard (e.g. standard Suricata) rules are used. You need R&E specific ones!



NikhefSOC setup: Jouke Roorda, Daniel Geerts, Sil Westerveld
based on evolved WLCG SOC concepts

And remember to engage users – also an intel source!

From Nikhef CSIRT <security@nikhef.nl>

To davidg@nikhef.nl 2026-02-27, 10:05

Subject **Login of David Groep (davidg) to Nikhef from an unusual location: RWTHPHYS RWTHPHYS (eid is v89JVRP5gt)** S/MIME

[English follows Dutch]

Geachte David Groep,

U, of iemand die zich als u voordeed, heeft ingelogged vanaf onde
locatie. U ontvangt deze waarschuwing omdat het de eerste keer is
deze plek inlogde. Wilt u controleren of u het inderdaad zelf was
hiervandaan inlogde? En zo niet, ons - de Nikhef helpdesk op tele
zie onder - waarschuwen?

```
  Eerste verbinding op: Feb 27 09:37:45
  Verbinding vanaf:     RWTHPHYS RWTHPHYS
                        North Rhine-Westphalia, Germany (of omgev
                        134.61.106.83 (ext-106-083.eduroam.rwth-a
  Gebruikte dienst:     SOGo Sync (CalDAV, CardDAV)
```

Is de verbinding inderdaad door u gemaakt?

Is de verbinding inderdaad door u gemaakt?

- als dat NIET ZO IS:
  dan is er op uw account davidg@nikhef.nl waarschijnlijk ingebroken.
  Neem direct contact op met de Nikhef helpdesk, op telefoonnummer
  020 592 2200, of stuur een mail naar security@nikhef.nl

- was u dit WEL:
  u kunt deze mail negeren. U krijgt dan geen verdere meldingen
  van ons over onze diensten die u vanaf deze locatie gebruikt.

- WEET u het niet en is de verbinding recent (u bent nog op dezelfde plaats):
  als u op https://myip.nikhef.nl/ hetzelfde internetadres ziet als boven, dan
  is er niets aan de hand. De MyIP web site toont u details over uw huidige
  verbinding
    https://myip.nikhef.nl/

Heeft u nog vragen of opmerkingen, stuur die dan naar security@nikhef.nl

Bij voorbaat dank!
  Nikhef helpdesk en de computer security groep.
  https://www.nikhef.nl/security/

---------- v89JVRP5gt on lvp013wm ----

A question of *when*, not *if* – hence we run security challenges

Communication:

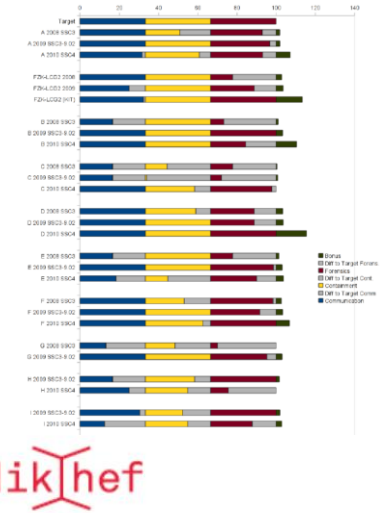
- Endpoints valid?
- Form/Content OK ?

Containment

- Ban ”malicious” users
- Find/Stop malicious processes
- Find submission IP

Forensics

- Basic Forensics on binary
- Network traffic



Nikhef

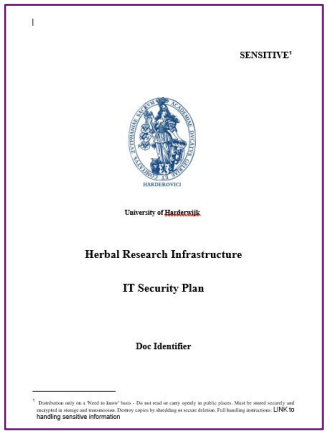
Nikhef CSIRT Traceability Challenge

Introduction

Deze Traceability Challenge bestaat uit drie onderdelen, in (naar verwachting) oplopende moeilijkheidsgraad. Iedere challenge begint met een externe 'trigger' – aan het eind van dit document staan de hints en de goede (of in ieder geval: de 'gewenste') oplossing.

Veel plezier!

Federation security table-top exercises


SENSITIVE[1]

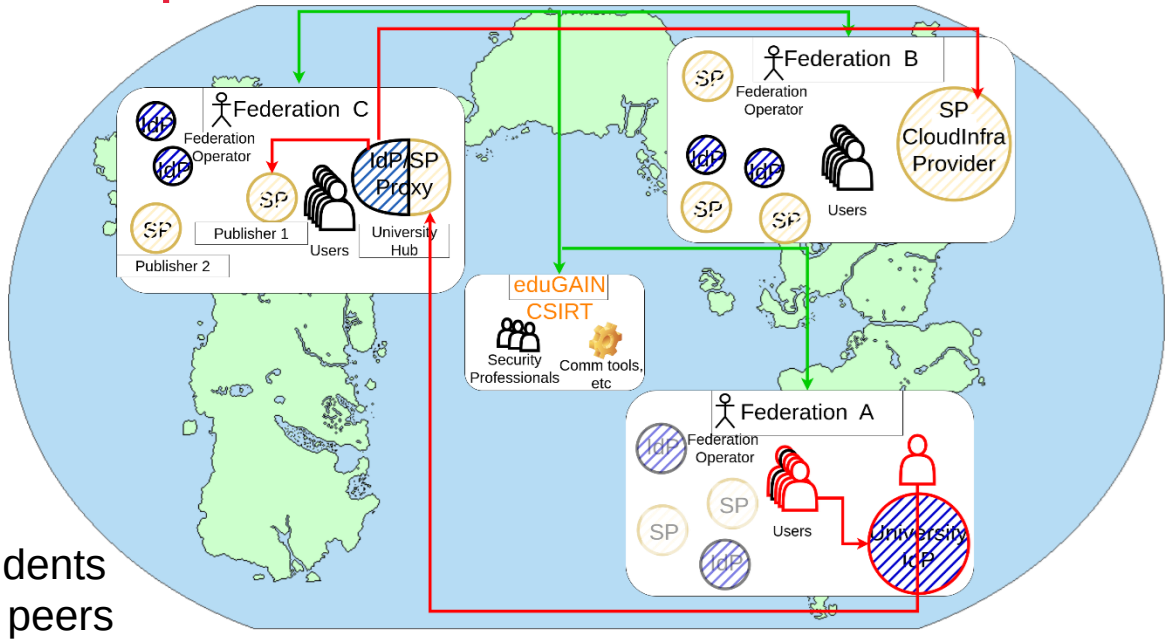
University of Hardervijk

Herbal Research Infrastructure

IT Security Plan

Doc Identifier

[1] Distribution only on a "Need to know" basis - Do not read or carry openly in public places. Must be stored securely and encrypted in storage and transmission. Destroy copies by shredding or secure deletion. Full handling instructions: LINK to handling sensitive information

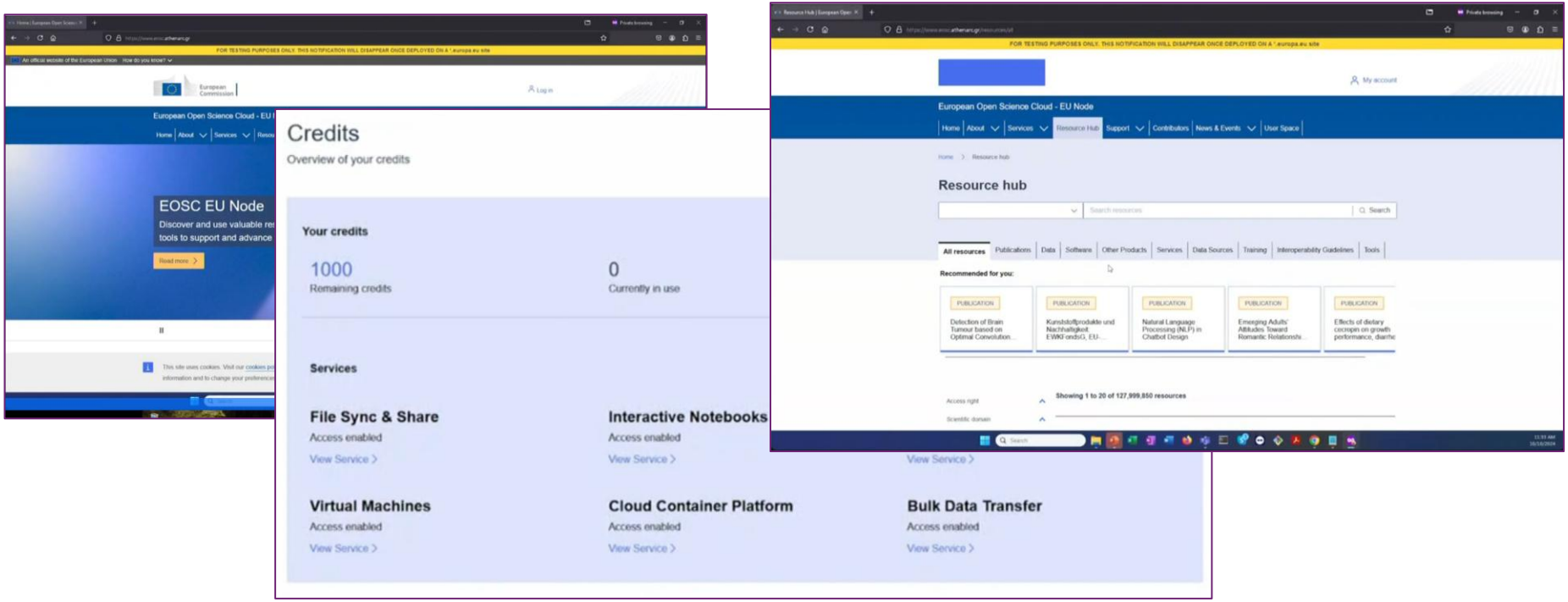


What your role play brings you ☺

- real time pressure to contain incidents
- true gratitude for protecting your peers
- collective recovery
- exploring some gruelling conflicts of interest!

eduGAIN TTX – role play scenario from the ISGC Security Workshop 2024, 2025

‘Global’ cross-domain services and catalogues are coming



https://webcast.ec.europa.eu/eu-node-technical-launch-event-24-10-10

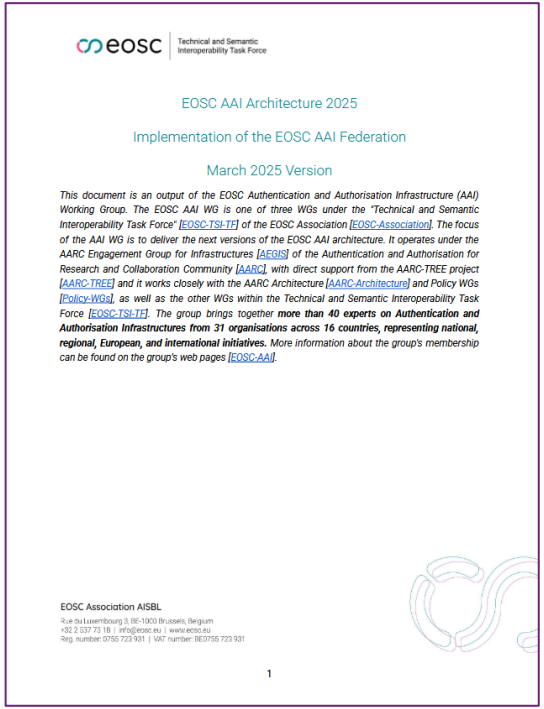
And security should be a *mandatory* corner stone

11. MUST support common security procedures

Security procedures define procedures and duties to allow an organised incident response. Distributed systems, in particular when spanning multiple organisational domains and countries, need a common approach for security related matters.

The following are well established in distributed infrastructures, and therefore mandatory for being supported:

- Security Incident Response Trust Framework for Federated Identity Sirtfi [REFEDS-SIRTIFI]
- Security Operational Baseline [AARC-G084] to enable secure infrastructure operation
- **Data Protection** for *access* to personal data: Compliance with the REFEDS Code of Conduct version 2 [REFEDS-DPCoCo] or other GDPR-aligned code of conduct.Collaboration Platform (Community AAI)



eosc | Technical and Semantic Interoperability Task Force

EOSC AAI Architecture 2025

Implementation of the EOSC AAI Federation

March 2025 Version

This document is an output of the EOSC Authentication and Authorisation Infrastructure (AAI) Working Group. The EOSC AAI WG is one of three WGs under the "Technical and Semantic Interoperability Task Force" [EOSC-TSI-TF] of the EOSC Association [EOSC-Association]. The focus of the AAI WG is to deliver the next versions of the EOSC AAI architecture. It operates under the AARC Engagement Group for Infrastructures [AEGIS] of the Authentication and Authorisation for Research and Collaboration Community [AARC], with direct support from the AARC-TREE project [AARC-TREE] and it works closely with the AARC Architecture [AARC-Architecture] and Policy WGs [Policy-WGs], as well as the other WGs within the Technical and Semantic Interoperability Task Force [EOSC-TSI-TF]. The group brings together ***more than 40 experts on Authentication and Authorisation Infrastructures from 31 organisations across 16 countries, representing national, regional, European, and international initiatives.*** *More information about the group's membership can be found on the group's web pages [EOSC-AAI].*

EOSC Association AISBL

Rue du Luxembourg 3, BE-1000 Brussels, Belgium

+32 2 537 73 18 | info@eosc.eu | www.eosc.eu

Reg. number: 0755 723 931 | VAT number: BE0755 723 931

1

EOSC AAI Architecture 2025 - Implementation of the EOSC AAI Federation; https://doi.org/10.5281/zenodo.15388270

So what do *you* do??

This work has also been co-supported by projects that have received funding from the European Union's Horizon research and innovation programmes under Grant Agreements GN5-1, GN5-2, EGI-ACE/EGI-Engage, EOSC Future, AARC/2, AARC TREE

This work is supported by SURF under the Innovation Programme, part of the NWO and SURF Execution Plan Digital Infrastructures for Research and other sources

David Groep
davidg@nikhef.nl
https://www.nikhef.nl/~davidg/presentations/
https://orcid.org/0000-0003-1026-6606

Maastricht University

Nikhef